NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ELECTRONIC WARFARE (EW) HISTORICAL PERSPECTIVES AND ITS RELATIONSHIP TO INFORMATION OPERATIONS (IO)—CONSIDERATIONS FOR TURKEY

by

Ali Can Kucukozyigit

September 2006

Thesis Advisor:	Daniel C. Boger
Second Reader:	Edward L. Fisher

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Electronic Warfare (EW) Historical Perspectives and Its Relationship to Information Operations (IO) – Considerations for Turkey			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kucukozyigit, Ali Can			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is the exploration of the relationship and interaction between Electronic Warfare (EW) and Information Operations (IO) core, supporting and related competencies. Understanding the definitions of information and its value, information superiority, and the decision making cycle provides the foundation for the thesis. Investigation of the historical transformation of EW from the U.S. Civil War to the First Gulf War, and also examining how the concept of IO has developed and evolved contributes to this study by helping to comprehend the modern day interaction between EW and each IO competency separately. This interaction is constructed upon the guidance and standards provided by the latest U.S. Joint Chiefs of Staff Publication Joint Publication 3-13 *Information Operations.*

This study concludes that the relationship between EW and IO is increasingly interactive and consists of two aspects: limiting and interfering, and reinforcing and supporting. Also, the relationship between EW and each IO competency is not consistent between the core and supporting competencies. In addition to these conclusions, this study expresses some considerations for EW and IO applications with respect to the unique environment and requirements of the Turkish Republic.

14. SUBJECT TERMS Information Operations, Electronic Warfare, History of EW, Turkey, Elektronik Harp, Bilgi Harekati, Bilgi Destek Harekati, Radar, IO Competency, EW relationship to IO, Information Superiority, OODA loop, ASELSAN, MILDEC, PSYOP, Information Technology,Public Affairs, Civil Military Operations, Physical Attack, Computer Network Operations,PSYOP, Harekat Guvenligi, Psikolojik Harp, Turkiye			**15. NUMBER OF PAGES** 169
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ELECTRONIC WARFARE (EW) HISTORICAL PERSPECTIVES AND ITS RELATIONSHIP TO INFORMATION OPERATIONS (IO) – CONSIDERATIONS FOR TURKEY

Ali Can Kucukozyigit
First Lieutenant, Turkish Army
B.S., Turkish Military Academy, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Ali Can Kucukozyigit

Approved by: Daniel C. Boger
Thesis Advisor

Edward L. Fisher
Second Reader

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is the exploration of the relationship and interaction between Electronic Warfare (EW) and Information Operations (IO) core, supporting and related competencies. Understanding the definitions of information and its value, information superiority, and the decision making cycle provides the foundation for the thesis. Investigation of the historical transformation of EW from the U.S. Civil War to the First Gulf War, and also examining how the concept of IO has developed and evolved contributes to this study by helping to comprehend the modern day interaction between EW and each IO competency separately. This interaction is constructed upon the guidance and standards provided by the latest U.S. Joint Chiefs of Staff Publication Joint Publication 3-13 *Information Operations*.

This study concludes that the relationship between EW and IO is increasingly interactive and consists of two aspects: limiting and interfering, and reinforcing and supporting. Also, the relationship between EW and each IO competency is not consistent between the core and supporting competencies. In addition to these conclusions, this study expresses some considerations for EW and IO applications with respect to the unique environment and requirements of the Turkish Republic.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAA	Anti-Aircraft Artillery
ARM	Anti-Radiation Missile
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System
BDA	Battle Damage Assessment
COMCAM	Combat Camera
COMINT	Communications Intelligence
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CI	Counter- Intelligence
CMO	Civil Military Operations
C2W	Command and Control Warfare
C^4ISR	Command Control Communications Computers Intelligence Surveillance Reconnaissance
CNO	Computer Network Operations
DEW	Directed Energy Weapons
DF	Direction Finder
DOD	Department of Defense
DSPD	Defense Support to Public Diplomacy
EA	Electronic Attack
ECM	Electronic Counter-Measure
ECMO	Electronic Counter-Measure Officer

EMCON	Emission Control
EMP	Electromagnetic Pulse
EOB	Electronic Order of Battle
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
EWO	Electronic Warfare Officer
GPS	Global Positioning System
HARM	High-speed Anti-Radiation Missile
HEL	High Energy Laser
HPM	High Power Microwave
IA	Information Assurance
IADS	Integrated Air Defense System
IED	Improvised Explosive Device
IMINT	Image Intelligence
INFOCON	Information Operations Condition
INFOSEC	Information Security
IT	Information Technology
IO	Information Operations
IW	Information Warfare
JDAM	Joint Direct Attack Munition
JRFL	Joint Restricted Frequency List
JSTARS	Joint Surveillance and Target Attack Radar System

MANPADS	Man-Portable Air Defense System
MASINT	Measurements and Signature Intelligence
MILDEC	Military Deception
NPS	Naval Postgraduate School
OODA	Observe, Orient, Decide, Act
OPSEC	Operations Security
PA	Public Affairs
PGM	Precision Guided Munition
PSYOP	Psychological Operations
RWR	Radar Warning Receiver
RHAW	Radar Homing and Warning
SAM	Surface-to-Air Missile
SIGINT	Signals Intelligence
TA	Targeted Audience
UAV	Unmanned Aerial Vehicle

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to recognize three groups of individuals whom I most sincerely acknowledge for their unforgettable and endless contribution to my success at the Naval Postgraduate School (NPS) in general and in particularly making this thesis a reality: my advisors, my family and friends, and the Turkish Military.

I would like to thank the Chairman of the Information Sciences Department and my advisor Doctor Dan C. Boger for his recommendations on whom to chose as my advisor and how to make my way through the thesis. Also, Mr. Edward L. Fisher deserves much praise for encouraging and guiding me even before my editor's review. Sir! You are one of the most—if not the most—patient individuals I have met in my life, thank you for your support. I would also like to present my thanks to my editor Valerie Haff for her contribution and insight into the thesis.

I must also acknowledge the infinite support and motivation of my sweet wife Duygu Kucukozyigit who did not even once complain about my long-lasting studies, both during my education at NPS and development of this thesis. I would like to thank CPT Aytug Denk and Lt.J.G. Aykut Kertmen for their sincere friendship and guidance through these past two years. They are true friends and deserve my gratitude.

As a proud officer who serves, I owe my success to the Turkish Armed Forces, for it has provided me with great educational opportunities throughout my career. Had the Turkish Army not chosen to send me here to study electronic warfare and systems engineering, I could have thanked none of the individuals above for their support in my studies, nor could I have taken pride in what I have accomplished so far.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Information dominance has been at the heart of military operations throughout history. In the information age the importance of information dominance and information superiority must be carefully addressed. Advanced technologies that are only a few decades old are now dramatically changing the way information is collected, stored, analyzed, and disseminated. The speed, accuracy, and timeliness of information has generated substantial research on these issues and ultimately stimulated the creation of the concept of *Information Operations* (*IO*). IO has many advantages over conventional operational concepts. Some of these advantages include, but are not limited to:

- IO can be applied throughout the full spectrum of peace, pre-conflict, conflict, post-conflict, and back to peace.
- IO is not only a military application; it is an entire process of decision making at every level, concerned with how to protect decision-making processes and influence adversaries in a desired manner.
- IO does not only impact military activities, but also has economic and politic aspects.
- IO can be utilized to avoid wars using core and related competencies, such as Defense Support to Public Diplomacy and Public Affairs.
- With IO, collateral damage can be minimized while still imposing objectives upon the adversary.

These advantages make IO increasingly relevant in the information age due to the variety of means IO uses to achieve the objective. It is important to keep in mind that IO is more about the objective than the means.

A. RESEARCH FOCUS

Understanding what information really is and its environment is critical to understanding the importance of information superiority, especially for leaders and decision makers. One research focus of this thesis is on the explanation of all of these concepts

Another research area examines the historical perspectives of Electronic Warfare (EW) from the U.S. Civil War through the First Gulf War. This research will present a historical synopsis of improvements in EW technology and its applications, and how they have been used during the major battles of the last century.

There are many studies available on Information Operations (IO) and its possible applications. However, there is no comprehensive study discussing how Electronic Warfare relates and interacts with each IO competency, whether core, supporting, or related. This thesis investigates the relationships between EW and twelve other competencies that are a part of, are related to, or support IO.

B. MAJOR RESEARCH QUESTIONS

This study will research the answers to the following questions:

- What is Information Operations (IO)?
    - What are the core, supporting, and related competencies of IO?
    - Why is IO gaining in importance?
- How did Electronic Warfare evolve in the last century?
- What is information?
    - What is the information environment?
    - Why is information important for military operations?
    - What is information superiority?
- Is there a difference between command and control warfare (C2W), Information Warfare (IW), and Information Operations?
- What is the relationship and interaction between EW and the IO competencies?
- How might the principles and theory behind IO be best applied to the needs of the nation of Turkey and its military?

C. KEY DEFINITIONS

Understanding the following important terms helps to better discuss the issues within this thesis.

Information: Facts, data, or instructions in any medium or form. Information also refers to the meaning that a human assigns to data by means of the known conventions used in their representation (Joint Publication 1-02, 256).

Information Operations (IO): IO are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own (Joint Publication 3-13, I-1).

Information Warfare (IW): Information Operations that is conducted during time of crisis or conflict to achieve or promote specific objectives over an adversary.

Information Superiority: A state of balance in one's favor in the information domain (Joint Vision 2020, 8) or the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (Joint Publication 1-02, 257).

Information Environment: The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (Joint Publication 1-02, 257).

Electronic Warfare (EW): In military operations, the term EW refers to any military action involving the use of electromagnetic energy or directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic Warfare includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES) (Joint Publication 3-51, I-1).

Electromagnetic Environment: The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of

electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static (Joint Publication 1-02, 175). The electromagnetic environment is the environment in which electromagnetic energy resides.

D. IMPORTANCE AND BENEFITS OF THE STUDY

Although this thesis is very comprehensive and electronic warfare-focused, many technical details and formulations are not included. The reason is that the study is intended to be easily understandable by non-engineers and other non-technical individuals with little or no EW or IO training, education, or background. This will benefit the study by broadening the targeted readers available.

This thesis will serve to broaden decision makers' understanding of the activities in the information age concerning information operations. It lays out the importance of information and the value it has, and also information superiority and its impact over both the adversary and friendly decision-making processes, which is the ultimate objective of information operations activities. A historical look at the evolution of electronic warfare and its impact on military activities will assist military leaders to appreciate the importance of this discipline. At the same time, this study will cover the birth and evolution of information operations ideologies.

Other studies of EW, and more recently of IO, have been done. However, none of them depicts the individual relationships of EW with each IO competency. This thesis will endeavor to explore these relationships and interactions, providing a unique contribution to literature in the field of study.

One other important aspect of this thesis is that it adapts information operations and electronic warfare to the particular environment of Turkey and discusses some considerations on the advancement Turkey has already made, and is yet to make, in these areas. This is an effort to improve the effectiveness and efficiency of Turkey‘s efforts in IO and EW.

The Interviews with two Naval Postgraduate School (NPS) faculty members on Information Operations and the Wild Weasel EW mission will help to describe and

increase comprehension of Information Operations concepts, and will serve to discuss the Wild Weasel mission from a first-hand perspective.

E. ORGANIZATION OF THE THESIS

This thesis consists of six chapters and three appendices. A flow for the thesis is presented in Figure 1 for easy visualization.

Chapter I presents an introduction to the entire thesis. It also asks the major questions to be answered and comments on the importance and benefits of this thesis.

Chapter II establishes an understanding of information and its value, the information environment, and information superiority. Also it investigates the importance of information for military operations.

Chapter III introduces IO and EW concepts and definitions in depth. It defines each IO competency and each EW discipline, which helps with the exploration of the interaction between IO and EW.

Chapter IV emphasizes the historical perspective of Electronic Warfare. It investigates some of the major conflicts, from the U.S. Civil War to the First Gulf War, from an EW perspective. In this chapter the birth and evolution of IO as a concept, along with the differences between command and control warfare (C2W), information warfare (IW), and IO are also addressed. This chapter lays out the vital role that EW plays in conflicts and its increasing importance for information systems and actions.

Chapter V focuses on how each of the IO competencies interacts with EW and explores the mutual relationship between each of them. This chapter evaluates each IO competency from its relationship to electronic warfare, which might be either limiting or reinforcing, or both.

Chapter VI emphasizes the considerations of IO and EW for the Turkish Republic and discusses some possible applications of IO and EW with respect to the specific environment of Turkey. This chapter also concludes the study and provides recommendations for further research.

The appendices include interviews with two Naval Postgraduate School faculty members about IO concepts and the “Wild Weasels.” The Wild Weasel concept is

important because it shows how tactics drive the technology, and the significance of melding technology and military tactics together in the same pot against an adversary.

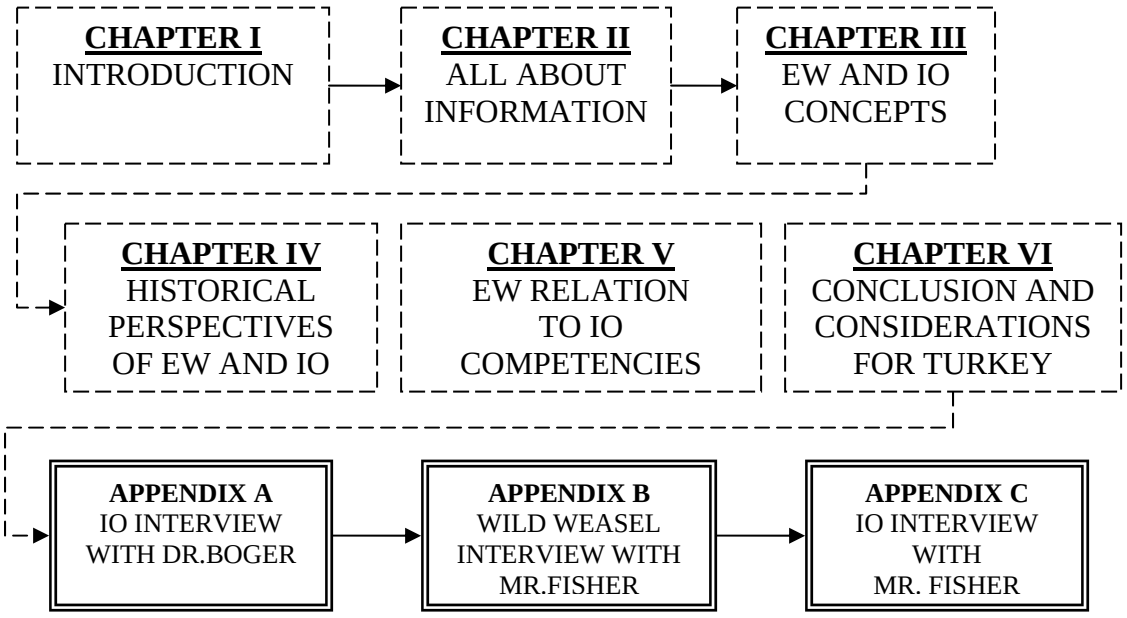


Figure 1. Organization of the Thesis Flow

II. INFORMATION

A. BACKGROUND

It is no secret that possessing the right information at the right time, in the hands of the right people, provides a crucial advantage for individuals, organizations, and nations. There has been a continuous struggle to acquire valuable information about adversaries while protecting information about ourselves. At the same time information should not be perceived as only a strategic phenomenon, it is also important at operational and tactical levels for planning and execution purposes. The struggle to acquire valuable information can take the form of economical, political, or military efforts. With the advent of the technical revolution in collecting, storing, analyzing, and disseminating data, beginning in the 1970s, the conduct of warfare has significantly changed. The first widely noted impact of this information revolution that affected the way a war was fought was exhibited during Operation DESERT STORM, or the First Gulf War.

1. How is Information Defined?

As stated in Joint Publication 3-13, *Information Operations*, information is a strategic resource vital to national security, and military operations now frequently depend on information and information systems for many simultaneous and integrated activities. It is difficult to explain information operations or any information-related activity without properly understanding the definition of information. Information is described as the facts, data, or instructions residing in some kind of medium or form. It is also defined as the meaning that a human assigns to data by means of the known conventions used when representing that data (Joint Publication 1-02, 256). Information is a term commonly used to refer to many points on the spectrum from raw data to knowledge, as seen in Figure 2. But in its most basic meaning, information is the result of putting individual observations, sensor returns or data items, into some meaningful context (Alberts 2001, 16).

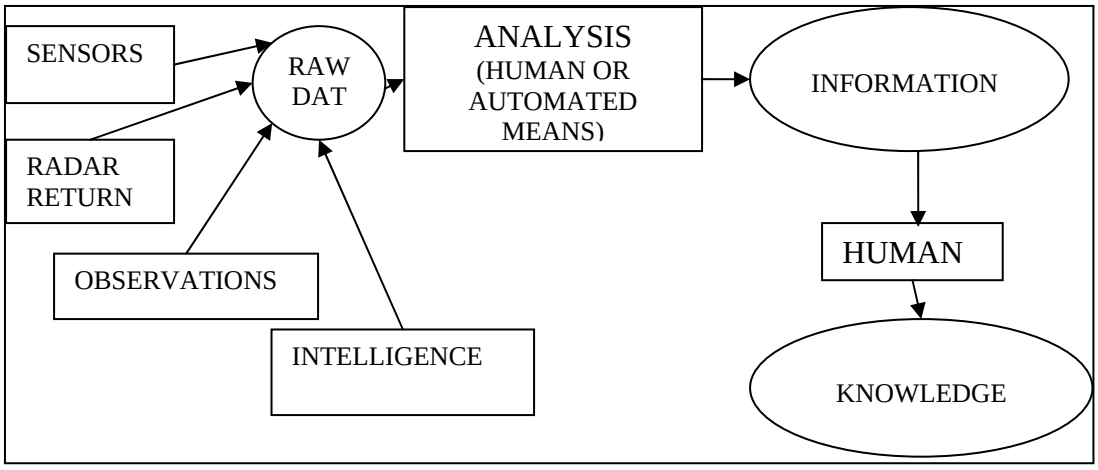


Figure 2. The Process of How Raw Data Becomes Knowledge.

Data is the representation of facts, concepts, or instructions in a formalized manner. Data should be suitable for communication, interpretation, or processing by humans or by automatic means (Joint Publication 1-02, 140).Radar returns, human observations, and other sensor inputs can be considered as data. It should be remembered that information and knowledge do not necessarily mean the same thing. Available information suggests conclusions drawn from patterns and leads to knowledge. "Knowledge of the situation can be drawn from conclusions that can be drawn from information about, for example, the types and locations of battle space entities" (Alberts 2001, 17).

2. Understanding the Information Environment

The information environment is an "aggregate of individuals, systems and organizations that are able to collect, process, disseminate or act on information" (Joint Publication 3-13, I-1).According to this definition, not only the systems and equipment that manipulate information, but also the decision makers, or individuals, should be considered as a part of the information environment. Humans and automated systems observe, orient, decide, and act (OODA) upon information in the information environment according to the well known OODA loop decision cycle. Therefore, the information environment is the principal environment of the decision making process. Although the information environment is considered distinct, it still resides within each of the four domains: sea, land, space, and air (Joint Publication 3-13, I-1). To better understand the information environment it is best to review its three dimensions. Figure 3

depicts the three dimensions of the information environment, which are the physical dimension, the information dimension, and the cognitive dimension.

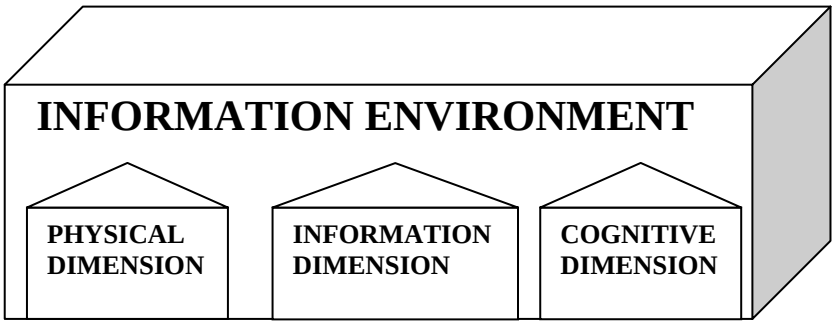


Figure 3. Three Dimensions of the Information Environment

The physical dimension is the first dimension where physical platforms and communications networks reside. Elements in this dimension are easy to measure, so combat power is conceptually measured here. The physical dimension can also be considered as ground truth or reality (Alberts 2001, 12). “Command and control systems, and supporting infrastructures that enable individuals and organizations across air, land, sea and space domains, reside in the physical domain” (Joint Publication 3-13, I-1).Examples of the physical dimension might be people, places, and capabilities like geographical coordinates and communications infrastructure.

The second dimension is the information dimension, where the information resides. The information is created, manipulated, and shared here (Alberts 2001, 12). More precisely, activities like collection, storage, display, and protection of information are all performed in this dimension. The information dimension is where modern military forces communicate and the commander’s intent is conveyed. It consists of “content and flow of information that must be protected” (Joint Publication 3-13, I-2). Examples include but are not limited to, context and content, usage of information capabilities, and networks of human-to-human contact.

The third dimension is the cognitive dimension. This dimension is considered to be the most important among the three because it is the dimension in which wars are actually won or lost. The cognitive dimension is described as the minds of participants where perceptions, beliefs, biases, quality of education, leadership, and morale exist, and

where decisions are made using these. Cultural and social factors, identity, and credibility of key decision makers are examples of the cognitive domain. As these features change from person to person, personal cognition of the world also changes. That is why it is difficult to measure the effectiveness of manipulation of the cognitive domain and to establish a set of standard rules for success in this area (Alberts 2001, 13).

In recent years, advanced technology has made it easy to manipulate the data in the information and physical dimensions. As it is easier to store, manipulate, and disseminate the data, it is more vulnerable to exploitation. On the other hand, the cognitive dimension is still not readily vulnerable to exploitation because recent technology still can not change people's beliefs and biases easily. Therefore, the side that can manipulate the cognitive domain is likely to succeed in obtaining information superiority. Figure 4 shows the three information environment dimensions and their characteristics.

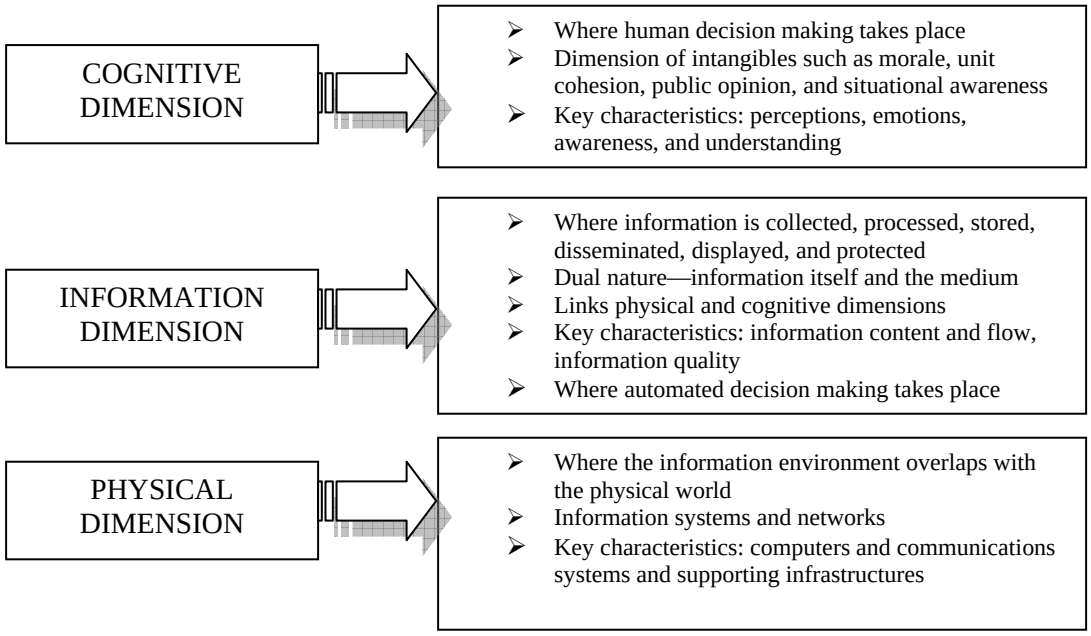


Figure 4. Dimensions of the Information Environment (After Joint Publication 3-13, I-2)

3. Information Superiority in Information Operations (IO)

Information superiority is transitory in nature and must be created and sustained through the conduct of information operations. However, the creation of information superiority is not an end in itself. Information superiority provides a competitive advantage only when it is effectively translated into superior knowledge and decisions. One must be able to take advantage of superior information converted to superior knowledge to

> achieve "decision superiority"—better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission (Joint Vision 2020, 8).

It is helpful to understand what information superiority means in order to better conduct information operations and to be able to make better decisions than an adversary. In Joint Publication 3-13, the principal goal of information operations is stated as "achieving and maintaining information superiority" (IX), which provides the commander an advantage only when it translates into superior decisions. Information superiority is a state of balance in one's favor in the information domain (Joint Vision 2020, 8). This can be accomplished by getting the right information to the right people at the right time in the right form, while denying an adversary the ability to do the same.

Trying to gain information superiority is not a new concept. Commanders and leaders have always tried to do so, and those who have gained this advantage have had significant success against the enemy. Sun-Tzu was a profound thinker who was able to lay out some of the basic fundamentals of gaining information dominance over the enemy, now called Information Operations (IO).

Normally, information can be considered independent from technology. But it should be remembered that acquiring, processing, and disseminating information has become very dependent on technology. For this reason, technology is a big contributor to information superiority if it can be used correctly (Fogleman and Widnall 1995, 2).

B. WHY IS INFORMATION ESSENTIAL TO THE MILITARY?

It would be wrong to consider information as a critical element only in the political and economical context. Information has always been at the center of military operations throughout history and will continue to be so. Many centuries ago Sun-Tzu emphasized the role of information and knowledge in warfare saying, "Know your enemy and know yourself; in a hundred battles you will never know peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If you are ignorant of both your enemy and yourself, you are certain in every battle to be in peril."(Sun Tzu 2002, 51) This is a famous and widely known quote from Sun-Tzu underlining the importance of information in warfare. This saying describes the basic

fundamentals of Information Operations. Information Operations (IO) is about knowing ourselves and denying that information to the enemy, or trying to know the enemy better in order to exploit their vulnerabilities. Sun-Tzu stated this concept about twenty-five centuries ago.

Individuals at all levels of military service must comprehend the vitality of information and act accordingly. It is also useful to understand the reasons information is essential for the military. Due to its complicated nature, there is always some uncertainty in a military environment about where the friendly and enemy forces are, what capabilities and intentions they have, and other things of this nature. In order to prevail against this uncertainty, leaders from the top to bottom levels need to gain information about the enemy and the battlespace. Only with timely and accurate information can a decision maker consistently come up with the correct action.

Determining the correct action has been very difficult to accomplish until recently. Modern advances in technology, in a general sense compared to older technologies, now provide the commander with a great deal of information to understand, analyze and act upon according to what is happening on the battlefield. Despite this, there will always be a significant level of residual uncertainty that will persist (Alberts 2001, 37). This is inevitable by nature. Even on the battlefield of the future it will probably be impossible to eliminate all uncertainty. The uncertainty might occur due to the flaws and imperfections of sensors, the differences in human perceptions, and many other potential reasons. Therefore, the side which makes the fewest errors manipulating the information will probably make better and healthier decisions and prevail.

Advances in technology have increased the complexity of information collection, processing, and dissemination; there is a great concern about how this will change the way wars are fought and the role it will play in transforming the tactics on the ground and the unit structure. In the interview located in Appendix B, Mr. Fisher stated “it is important not to have technology drive military tactics. If we are complacent with technology, then someone smarter than us might go ahead and develop new tactics and weapons that surprise us and catch us off-guard”. In this sense, it is essential for each and

every individual in the military to understand the role of technology and information in depth so that he or she can carry out missions effectively.

If countries can not be successful in the adopting a comprehensive and disciplined process when confronted with these technologies, the positive potential that they possess can not be realized. In such case, there is high likelihood that negative impacts might reach to unacceptable limits. The solution to this problem is co-evolution of concepts, doctrines, organizational structure, training, and new technology. To perform this task in the battlespace effectively requires understanding the value and importance of information. Information has a great impact on transforming military equipment and operations by providing commanders with a large quantity and quality of information. Thus the commander has the advantage over the adversary of observing and analyzing the battlespace and communicating a decision to the forces with quality information (Fogleman and Widnall 1995, 2).

Information is a strategic resource that is critical for military operations and the security of nations. With the uncertainty and complexity of the battlespace, military operations are incredibly dependent on information and information systems to integrate, coordinate, and synchronize activities. This introduces military decision makers to another challenge: the same tools the military uses, such as the Public Affairs, Psychological Operations, the Internet, and modern media, can be used by adversaries and might cause a significant adverse impact on the military environment, because they are available to almost everyone around the globe (Joint Publication 3-13, I-4). They are cheap to obtain, commercial-off-the-shelf (COTS), and easy to establish and sustain. They do not require a high level of expertise. This perspective contributes to the importance of information for military operations.

Another contribution that information makes is during the planning process. To plan operations professionally, military decision makers should study and understand the importance of information for operations because the desired effect of information operations is not always to fight and destroy the enemy. Each military operation necessitates different goals in terms of IO. In humanitarian assistance, for example, the

end result should be winning the “hearts and minds” of the targeted audience (TA). Only a commander who can understand the impacts and desired end effects of information in depth can make appropriate decisions.

In addition, understanding the importance of information in depth will enable the commander to visualize the information operations capabilities of the adversary and take the necessary precautions to prevent friendly information from compromise by the enemy. The continuously changing nature of the combat zone actually adds more complexity to the processing of information and thus makes understanding information even more difficult (Joint Publication 3-13, I-4).

C. MEASURING THE QUALITY OF INFORMATION

The quality of information is important in any kind of operation. Nevertheless it is very difficult to measure and in most cases almost impossible. The quality criteria for information are shown in Figure 5. However different goals for the use of information require different application of these criteria as well as a different weighing of each criterion (Joint Publication 3-13, I-3). For every particular case, some of these criteria might be omitted or applied in varying weight. In any case, they play important roles in being able to get the right information, at the right time, in the hands of those who need it.

As we don’t have a means to measure the quality of information before it is obtained, the quality often is subjective. It changes according to the cognitive dimension of the particular individual, his or her biases, education, training, morale, and experience. From this perspective Information Operations is very different from conventional warfare targeting and kinetic weapons where measuring the effectiveness of the tools is easier using physical measures.

ACCURACY	**Information that**	conveys the true situation
RELEVANCE		applies to the mission, task, or situation at hand
TIMELINESS		is available in time to make decisions
USABILITY		is common, in an easily understood format
COMPLETENESS		provides the decision maker with all necessary data
BREVITY		has only the level of detail required
SECURITY		has been afforded adequate protection where required

Figure 5. Quality Criteria of Information (After Joint Publication 3-13, I-3)

D. WHAT IS THE OODA LOOP?

As mentioned above, all Information Operations efforts concentrate on decision-making processes. The ultimate IO objective is to influence the adversary decision making cycle and the same time protect the friendly. One of the methodologies used to understand decision-making processes is Observe-Orient-Decide-Act (OODA). OODA is a theory that was developed by Col. John Boyd, a former U.S. Air Force officer. This process is critical not only for military commanders but also political leaders, or any individual who is in a position to make decisions.

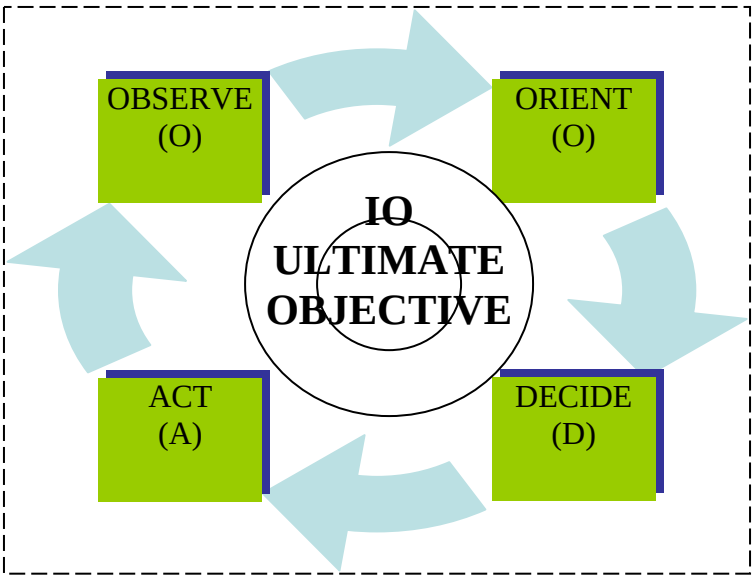


Figure 6. The Sequential Phases of the OODA Loop

In the OODA process, there are four phases: observe, orient, decide, and act. The OODA loop shown in Figure 6 is a process that ultimately creates an action for a specific situation. The continuity and completion of the loop must be sustained at all times in order to make healthy and correct decisions.

The OODA loop is important when making distinctions between different decisions. Many quick and reflexive decisions might not require all phases of the loop as they might be short-circuited. An example is a soldier who is quickly deciding whether he will shoot the enemy or not when they confront each other suddenly. In this example it is not wrong to say that the soldier is probably only using “observe” and “act” phases of the OODA loop since he or she does not have ample time to orient and decide. In other words observe and orient merge and become one phase, and decide and act likewise merge. Nevertheless, more complex decisions use each step of the decision cycle (Alberts 2001, 23). As the faces of the battles are changing due to technological developments, the decision makers’ need to the OODA loop increase.

Observation is the initial step in the OODA loop. A commander gathers information from all available sources, such as surveillance, reconnaissance, and target acquisition. The information collected in the observation step of the loop is converted into intelligence in the orientation step (Joint Publication 3-13.1, A-1). The inputs during

this phase are very important because actions carried out in the following phases will all depend on the data collected during the observation phase.

In the orientation phase the commander tries to understand the actual situation and environment of both sides (Joint Publication 3-13.1, A-1). This phase can be omitted for simple, reflexive decisions.

The decision phase is where the commander makes his decisions based on the assumed reality of the operational area (Joint Publication 3-13.1, A-1). This decision has to be conveyed through a robust communication medium to get to the receiver.

Finally, after reaching the decision, the commander takes action and actually impacts the operational area by his orders and instructions in the action phase.

In order to achieve information superiority and become successful in conducting IO, one should be able to get into the adversary's OODA loop by breaking it, slowing it down, and manipulating it so that it produces delays and incorrect actions. On the other hand, one should protect his or her OODA loop from hostile activities by hiding it from enemy information collection activities, keeping the cycle unbroken and robust, making it act faster than the enemy's cycle, and sustaining the health of the OODA loop so that it produces appropriate and timely decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INFORMATION OPERATIONS AND ELECTRONIC WARFARE

Chapter V investigates one of the focus areas, the interaction and mutual relationship between each Information Operations (IO) competency and Electronic Warfare (EW). In order to understand these features, one must first understand the IO concept and be familiar with types of EW activities and subdivisions (disciplines). This chapter establishes a pathway to understanding IO-EW interactions by studying each competency and EW subdivision.

A. WHAT IS INFORMATION OPERATIONS (IO)?

1. Defining Information Operations

Information Operations is defined as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own" (Joint Publication 3-13, I-1). These components are considered as the major players in an Information Operations campaign. Electronic Warfare is omitted in this section as a core competency because it is discussed in detail in the following section.

IO supporting capabilities—information assurance (IA), physical security, physical attack, counter-intelligence (CI), and combat camera (COMCAM)—directly or indirectly contribute to the effectiveness of IO. IO-related capabilities include public affairs (PA), civil military operations (CMO), and defense support to public diplomacy (DSPD) (Joint Publication 3-13, I-6). All core, supporting and related competencies can be seen in Table 1.

The primary purpose or objective of IO related capabilities should not be compromised by IO; they should be coordinated and synchronized with the core and supporting IO competencies.

CORE COMPETENCIES	Psychological Operations (PSYOP)
	Military Deception (MILDEC)
	Operations Security (OPSEC)
	Electronic Warfare (EW)
	Computer Network Operations (CNO)
SUPPORTING COMPETENCIES	Information Assurance (IA)
	Physical Security
	Physical Attack
	Counter Intelligence (CI)
	Combat Camera (COMCAM)
RELATED COMPETENCIES	Public Affairs (PA)
	Civil Military Operations (CMO)
	Defense Support to Public Diplomacy (DSPD)

Table 1. Information Operations (IO) Competencies (After Joint Publication 3-13, I-6)

2. Core Competencies of IO

There are five core competencies of Information Operations, as seen in Figure 7. The core competencies are the major components in the conduct of IO; however, they should not be perceived as separate tools that can, by themselves, realize IO objectives. Instead, they should be considered as tools that allow an IO campaign to succeed by synchronizing, coordinating, and integrating with the other core, supporting and related competencies. Well-coordinated related and supporting competencies reinforce the power and increase the effectiveness of the core competencies.

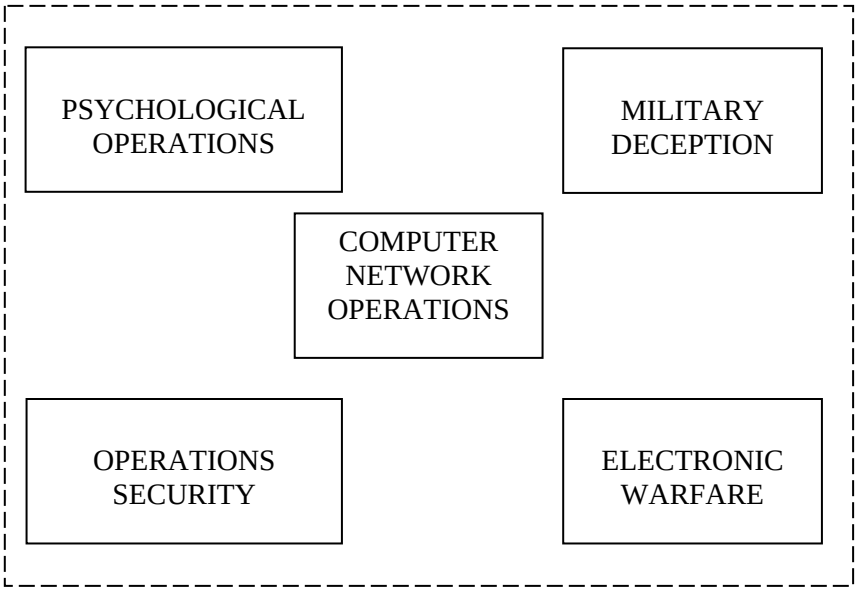


Figure 7. IO Core Competencies

a. Psychological Operations (PSYOP)

Psychological operations have an important role in military operations. Mao emphasized that importance by indicating the mind of the enemy and the will of his leaders as a target that is much more important than the bodies of the troops they have As the purpose of psychological operations is to influence foreign decision makers to decide in friendly favor, it definitely makes a critical contribution beyond the normal kinetic goal of killing enemy soldiers. Psychological operations are defined as "planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals; and the purpose of PSYOP is to introduce or reinforce foreign attitudes and behavior favorable to the originator's objectives" (Joint Publication 3-13, II-1). This can be achieved using appropriate means, such as radio, print, or other media. The advances in communication capabilities have also enhanced PSYOP means, but the effectiveness achieved is dependent on how the targeted audience perceives the message and on the credibility of that message. Figure 8 shows the essentials for a successful PSYOP campaign (Joint Publication 3-53, I-1). Though they can be successful, PSYOP are not easy to conduct, because there are uncontrollable complex variables that have many potential impacts on PSYOP efforts,

like enemy counter-PSYOP activities effects, public affairs effects, and many others. Another important issue is the analysis and evaluation of the campaign. It is never easy to get the results of a PSYOP campaign; the results are not concrete, are mostly qualitative and typically require long periods of time to be observed.

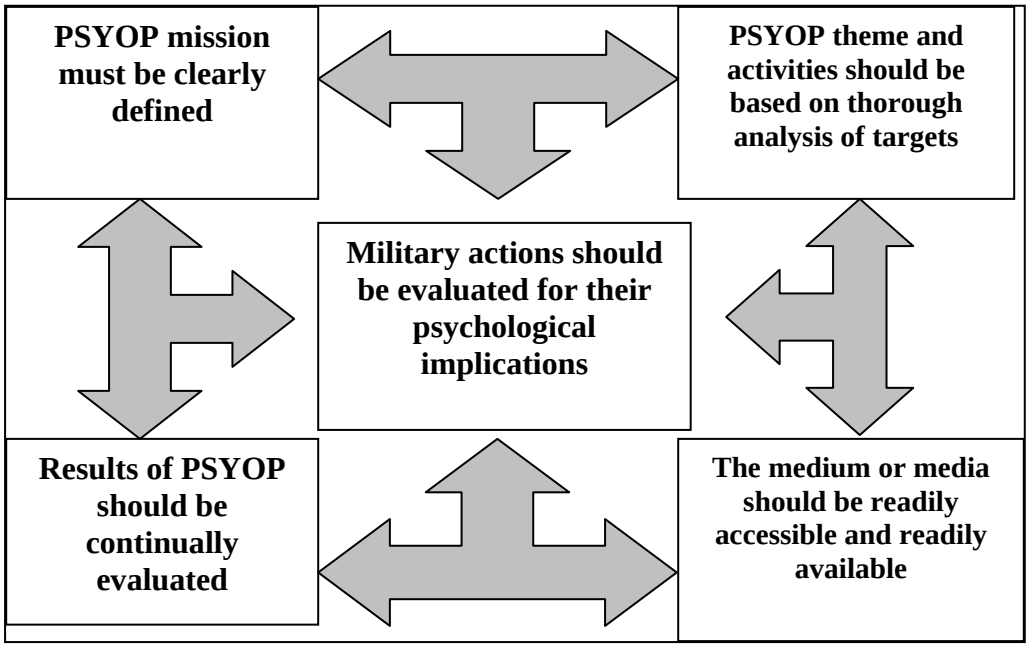


Figure 8. Essentials of Success in a PSYOP Campaign (After Joint Publication 3-53, 13)

Due to the improvements in the communication means that are used when conveying PSYOP messages, it is increasingly likely to influence strategic audiences when making efforts at the tactical level. Communication mediums have facilitated reaching individuals at the very bottom level, such as radar operators and artillery personnel. They have introduced more means more powerful and immediate than radio broadcasting, leaflet bombs, and loudspeakers. The Internet and satellite broadcasting are examples of these new and powerful communication tools.

b. Military Deception (MILDEC)

Military Deception is one of the oldest tools used in the history of military action; an example is the Trojan Horse myth. According to an ancient Greek mythology, the Greeks defeated the Trojans by deceiving them with a giant wooden horse, presented as a gift. The Trojan's accepted the gift into the city of Troy. The Greeks had placed men

inside the wooden horse. These men snuck out at night and opened the gates to the city, allowing the Greek army to enter Troy and defeat the Trojans.

Looking at recorded history, deception played a critical role in the success of the Normandy invasion, as it caused the German command to make many critical errors in judgment (Joint Publication 3-58, I-2). The Allies used operations security, electronic deception, and fake military operations to support the Normandy invasion. These and other actions convinced the Germans to believe the intentionally conveyed themes, and thus to make incorrect decisions on Allied intentions and objectives due to a false visualization of the battlespace.

Military deception is defined as the "actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions, or inactions that will contribute to the accomplishment of the friendly mission" (Joint Publication 1-02, 334). Sun-Tzu expresses the importance of military deception in warfare by saying "all warfare is based on deception" (Sun Tzu 2002, 42). The principles of military deception as presented in Table 2 are focus, objective, centralized control, security, timeliness, and integration.

FOCUS	Targeting the adversary's decision-making process
OBJECTIVE	To cause the adversary to take specific action, not just to believe something
CENTRALIZED CONTROL	A deception must be controlled and directed by a single element; however, execution may be decentralized
SECURITY	Need-to-know criteria must be applied to each deception effort
TIMELENESS	Deception requires careful timing
INTEGRATION	MILDEC must be fully integrated and occur simultaneously with the operation planning

Table 2. The Principles of Military Deception (After Joint Publication 3-58, p. I-3)

The application of military deception goes back to the early stages of conflict history. In his book *The Art of War*, Sun-Tzu said, "when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe that we are far away; when we are far away, we must make him believe we are near. Hold out baits to entice the enemy" (Sun Tzu 2002, 42). This tactic is still valid and is what decision makers pursue today. The principles of MILDEC do not necessarily change, but its application to battlespace changes concurrent with technological development and advances in communications and networking.

The goal of deception is to cause the adversary to make incorrect decisions. Deception does this by creating an apparent reality. Generally, this entails creating phenomena for the enemy to successfully observe. This, however, depends on several conditional events: the adversary actually observes the phenomenon, thereby turning it into data; analyzes it into the desired information; and acts upon the information in the desired manner (Fogleman and Widnall 1995, 5).

c. Operations Security (OPSEC)

By its definition OPSEC is "a process of identifying critical information and subsequently analyzing friendly actions and other activities to: identify what friendly information is necessary for the adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remain secure" (Joint Publication 3-13, II-3). It is clear in this definition that OPSEC is a process that can be applied to every operation, but should not be seen as a set of golden rules that provides security for military operations. It should be carefully studied in every operation concerning the specific requirements of that operation.

Operations security should not be confused with communications security (COMSEC) or information security (INFOSEC). It is the process of identifying friendly critical information and then analyzing friendly actions to decide which friendly actions can be observed by the adversary. Then, one can determine what kind of indicators adversary intelligence systems can obtain, assess timely critical information, and take the

necessary precautions in order to eliminate or reduce these to an acceptable level of vulnerability (Joint Publication 3-54, I-1).

d. Computer Network Operations (CNO)

Along with electronic warfare, computer network operations is a capability that has evolved recently and has become very popular in a short time period. The reason for this is the increasing use of networking and information technologies (IT) infrastructure in military and civilian organizations. To attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructures, CNO is comprised of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE).

Computer network attack is actions to disrupt, deny, and destroy information using computer networks. In some cases these actions might target the information within the network or computer, or the physical network or computer themselves. The purpose of computer network defense is to protect, monitor, detect, and respond to unauthorized activity within a specific network. Computer network exploitation involves actions taken to gather data from adversary automated information systems or networks (Joint Publication 3-13, II-5).

Information Assurance (IA) is a very important part of computer network operations. It plays a major role in protecting computer networks and information technologies (IT) from hostile activities. IA focuses on the information itself, whereas computer network defense focuses on the machinery in which information resides. Therefore, IA and computer network defense are complimentary. In addition to adversary activities that threaten computer systems and networks, threats also come from hackers who attempt to access or contaminate sensitive information for fun.

Again, the final core competency of IO, electronic warfare, will be discussed at length in section B of this chapter.

3. Supporting Competencies of IO

There are four IO supporting competencies that contribute to the effectiveness of the core competencies, as seen in Figure 9. These competencies are information assurance (IA), physical attack, physical destruction, and combat camera (COMCAM).

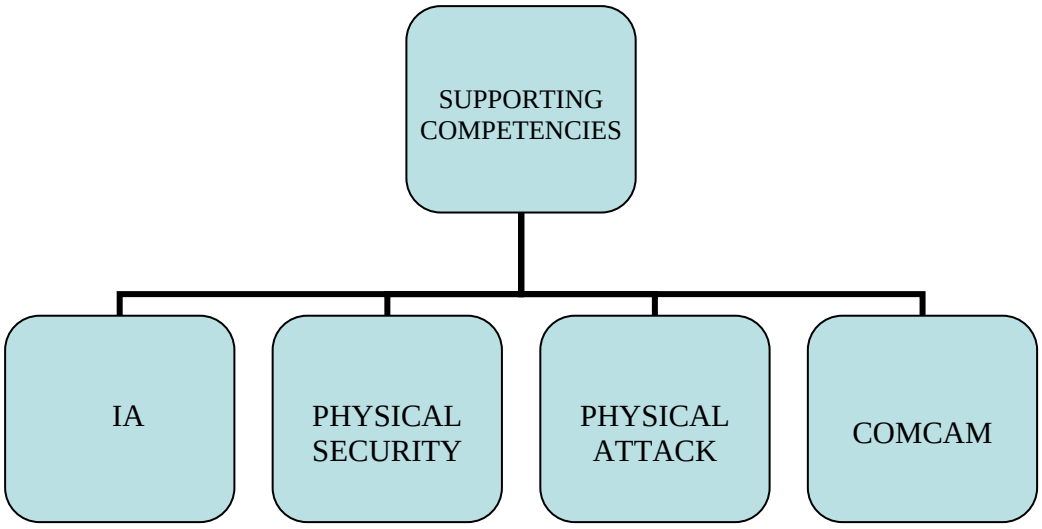


Figure 9. IO Supporting Competencies

a. Information Assurance (IA)

IA necessitates a defense-in-depth approach when integrating the capabilities of humans, operations, and technology. Defense-in-depth is based on the concept that multiple layers of security filling the gaps between them create greater security than can be achieved by any single protection mechanism. IA also helps establish a multilayer and multidimensional protection for mission accomplishment. IA is defined as "measures that protect and defend information and information systems by ensuring its availability, integrity, authentication, confidentiality, and non-repudiation" (Joint Publication 3-13, II-5). There is always a high possibility that information can be obtained from insiders. Even though series of multi-layered security systems can be established against an outsider, the vulnerability of the data being accessed by the insider still exists. There is always a possibility that even the most trusted employee or operator who is inside the network can still reveal the secret / secured data to outsiders

Being interrelated, computer network defense and information assurance always depend on each other for effectiveness. IA activities are also often closely integrated with electronic protection (EP) activities. Some instances may show overlap between specific IA, CND, or EP activities, but integration of these activities should always be accomplished to eliminate this overlap. Otherwise there is a possibly that they will limit each other's area of operation. The application of IA is inherent to all military activities at all levels of command.

IA also involves computer and communications security (COMPUSEC/COMSEC). Computer security is the measures and controls taken to ensure confidentiality, integrity, and availability of information processed and stored by a computer. Communications security is the measures and controls taken to deny unauthorized persons information obtained by means of telecommunications while also accomplishing their authenticity. It also includes crypto security, transmission security, emission security (EMSEC), and physical security of communications materials and information (Air Force Doctrine Document 2-5, 23).

b. Physical Security

Physical Security is one of the security measures that are taken against sabotage, damage, theft, and espionage to physically protect personnel, materials, and installations, and to prevent adversaries from gaining access to them. Physical security protects the means of possessing information and information systems physically, whereas IA protects information and information systems in the electronic environment. Determining vulnerabilities to known threats, applying appropriate deterrents, controlling and denying safeguard techniques and measures, and responding to changing conditions are also included in physical security. While IA protects and ensures the information itself, physical security protects the physical facilities in which information resides (Joint Publication 3-13, II-6).

Physical security measures should be applied in order to deter, detect, and defend against threats from terrorists, criminals, and unconventional forces. Some of the examples of physical security are fencing, lighting and sensors, vehicle barriers, intrusion detection systems, and electronic surveillance and access control devices and systems. It is important to use physical security measures, overlapped and deployed in depth (Joint Publication 3-57, III-8).

c. Physical Attack

Physical attack is fundamental to military operations; destructive power is used to disrupt, destroy, and damage targets. For example, physical attack can be used to partially destroy adversary command and control, forcing operations with alternative means that may be exploitable by electronic warfare support resources. Physical attack can influence a target audience to act in ways favorable to friendly forces. It can also be

employed to attack command and control (C2) nodes to affect the adversary's ability to carry out C2 missions (Joint Publication 3-13, II-7). Continuous physical attack also helps decrease the adversary's morale and will to fight. GPS-guided munitions, precision-guided munitions (PGM), and similar technologies should be used in order to minimize collateral damage.

d. Counter-Intelligence (CI)

CI is the information gathered and the activities conducted with the purpose of protecting against espionage, other intelligence activities, sabotage, or assassinations, which might be conducted by or on behalf of foreign governments, foreign organizations, foreign persons, or international terrorists" (Joint Publication 3-13, II-7). It is a critical part of protecting friendly information. A robust security program should be established using OPSEC, CI, and physical security.

e. Combat Camera (COMCAM)

COMCAM supports combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations for military purposes. To provide support, COMCAM acquires and utilizes still and motion imagery (Joint Publication 1-02, 97). COMCAM uses imagery in support of IO and can be intended to influence an adversary or support friendly forces (Joint Publication 3-13, II-8). COMCAM support is important when conducting visual battle damage assessment (BDA). COMCAM (see Figure 10) provides visualization of the battlefield and increases the credibility of Psychological Operations campaigns.

Figure 10. COMCAM Includes Still and Motion Imagery for Military Purposes (From Naval Media Center Website 2006)

4. Related Competencies of IO

There are three IO related competencies that contribute to the effectiveness of the core and supporting competencies. Figure 11 shows these three related competencies: civil military operations (CMO), public affairs (PA), and defense support to public diplomacy (DSPD). These competencies are significant to IO and must always be coordinated and integrated with the IO competencies.

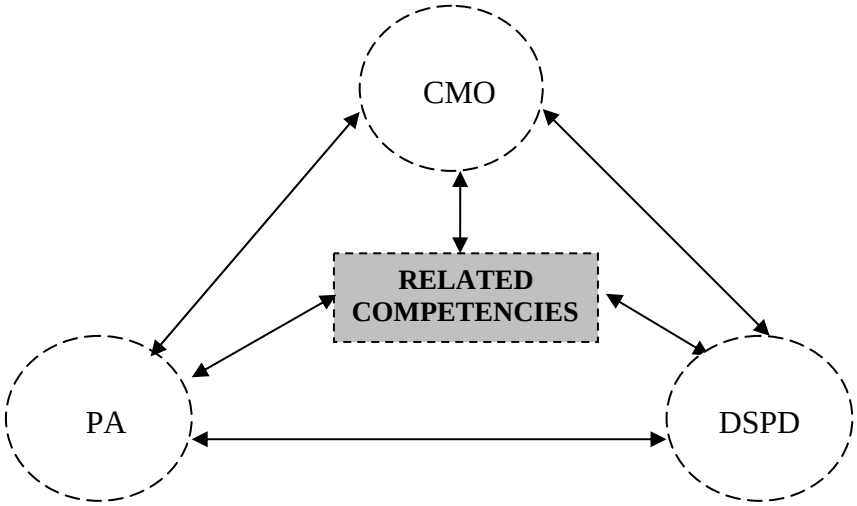


Figure 11. IO Related Competencies

a. Public Affairs (PA)

Public affairs is comprised of public and command information and community relations activities directed toward both external and internal audiences (Joint Publication 3-13, II-8). Credible public affairs is critical to the success of an overall IO campaign by influencing the adversary's decision-making process. If the adversary thinks the information conveyed by PA is incorrect, then it seeks other sources to verify the message conveyed through PA activities. This might delay the appropriate decision, and it is not what PA intends to accomplish. PA contributes to the success of a military operation by countering adversary misinformation and disinformation by publishing the real and accurate information (Joint Publication 3-13, II-9).

PA should not be confused with psychological operations. PSYOP aims to influence the adversary's decision to act or remain inactive, whereas PA aims to inform

the target audience (TA). There is a possibility that the enemy will use PA as an open intelligence source and act accordingly, however this is not the primary purpose of PA. This can be exploited by unknowingly conveying incorrect or deceptive information through PA channels. In addition, the internal audience should not be targeted with a PSYOP campaign, but PA can try to influence the internal audience through dissemination of accurate and timely information.

b. Civil Military Operations (CMO)

Civil military operations activities might take place before, during, or after a military operation and can include actions or functions which are normally the responsibility of the governing power in the area. Civil military operations are significantly due to the fact that they immediately affect the perceptions of the local populace. Civil military operations are defined as "the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace" (Joint Publication 3-13, II-9). Some of the civil military operations missions in support of regional conflict and other combat operations are shown in Figure 12.

The objectives of CMO are supporting national objectives, enhancing military effectiveness, and reducing the negative impact of military operations on society and civilian decision makers (Joint Publication 3-57, I-8). Civil military operations are conducted to minimize civilian interference with military operations and to maximize support for operations. CMO are conducted to meet the commander's legal responsibilities and moral obligations to civilian populations in the theater (Joint Publication 3-57, I-1).

Figure 12. Civil Military Missions in Support of Major Regional Conflicts and Other Combat Operations (From Joint Publication 3-57, I-10)

c. Defense Support to Public Diplomacy (DSPD)

The activities and measures taken in order to support and facilitate public diplomacy efforts are called defense support to public diplomacy (DSPD) (Joint Publication 1-02, 148). Defense support to public diplomacy helps promote foreign policy objectives by understanding, informing, and influencing foreign audiences and decision makers. It broadens the dialogue and cooperation among countries (Joint Publication 3-13, II-10). If used carefully, DSPD can be a great tool to help avoid conflict.

B. WHAT IS ELECTRONIC WARFARE (EW)?

1. Some Definitions Related to Electronic Warfare

It is useful to be familiar with the terms in this section in order to better understand the electromagnetic world. The definitions given here are also useful in understanding the relationships between the EW and IO competencies.

Electromagnetic Spectrum: The range of frequencies of electromagnetic radiation (Joint Publication 3-51, I-1). The electromagnetic spectrum is shown in Figure 13.

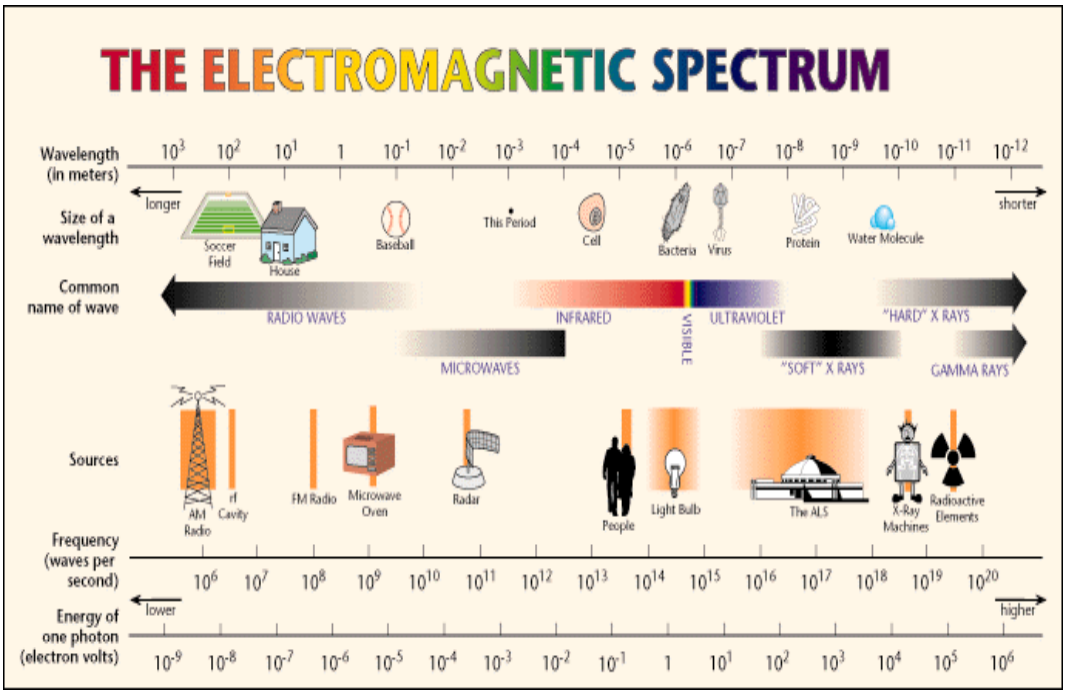


Figure 13. Electromagnetic Spectrum (From NASA Official Website 2006)

Operational Electromagnetic Energy Operational electromagnetic energy is a combination of the power, frequency, and duration of the electromagnetic emissions that may be encountered by a military force while performing its assigned mission (Joint Publication 3-51, I-1).

Directed Energy (DE) DE is a general term that defines the technologies relating to the production of a beam of concentrated electromagnetic energy, atomic particles, or subatomic particles. It is used to damage or destroy an adversary's equipment, personnel, and facilities (Joint Publication 3-51, I-4). A laser that blinds the sensors of an adversary is an example of a DE weapon.

2. Defining Electronic Warfare

The first paragraph of the introduction to Joint Publication 3-51 explains the importance of EW as follows:

> Military operations are executed in an increasingly complex electromagnetic environment (EME). Today, electromagnetic (EM) devices are used by both civilian and military organizations for communications, navigation, sensing, information storage, and processing,

> as well as a variety of other purposes. The increasing portability and affordability of sophisticated EM equipment guarantees that the EME in which military forces operate will become more complex in the future. The recognized need for military forces to have unimpeded access to and use of the EME creates vulnerabilities and opportunities for electronic warfare (EW) in support of military operations. In joint operations, EW is one of the integrated capabilities used to conduct information operations (IO). (Joint Publication 3-51, I-1)

Electronic Warfare (EW) is defined as "any military action involving the use of EM or directed energy to control the EM spectrum or to attack the enemy" (Joint Publication 3-51, I-1). EW has three subdivisions: electronic protection (EP), electronic warfare support (ES), and electronic attack (EA). Figure 14 depicts the conceptual view, interrelation of subdivisions, and relationship of subdivisions to principal EW activities. These three activities are sometimes referred to as 'electronic warfare disciplines'.

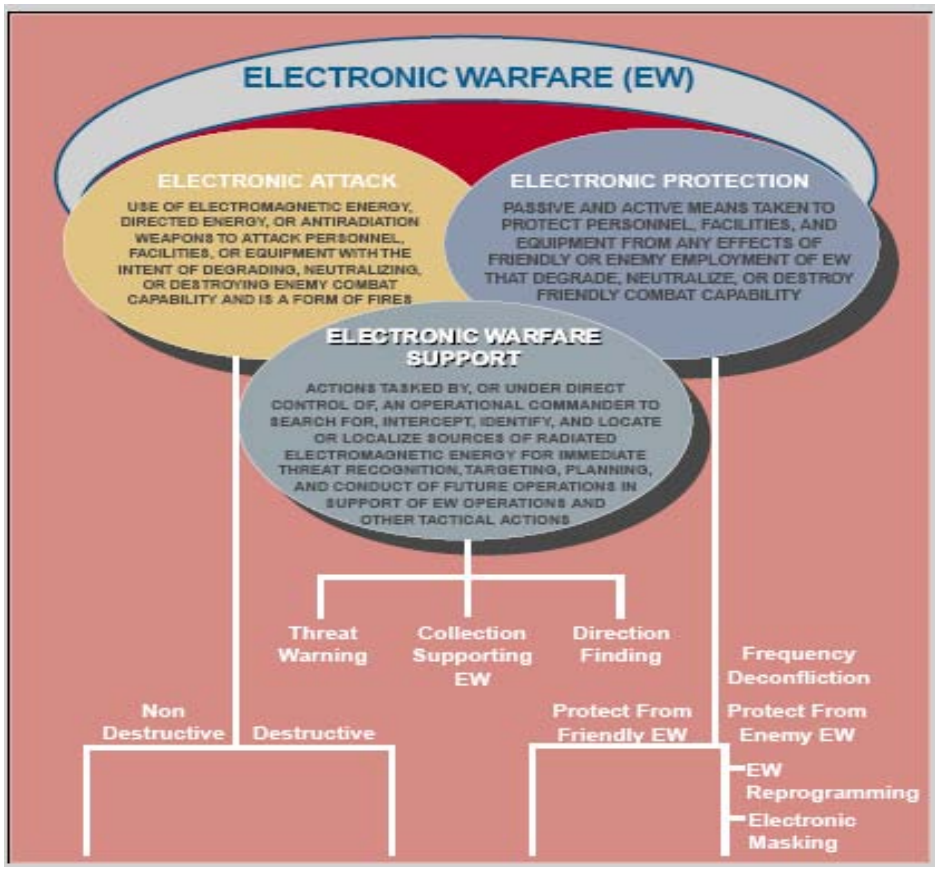


Figure 14. Concept of Electronic Warfare (From Joint Publication 3-51, I-3)

3. The Major Activities Performed in EW

The principal activities of EW basically exploit the opportunities and vulnerabilities that the physics of electromagnetic energy dictate (Joint Publication 3-51, I-5). The capabilities shown in Table 3 are the basic capabilities that are used in the realm of EW. These capabilities should be well-coordinated and integrated to achieve the ultimate objective of the EW mission and final military campaign. Appropriate capabilities to a specific operation might be used individually or in concert.

1	EM Compatibility (EMC)	9	Electronic Probing
2	EM Deception	10	Electronic Reconnaissance
3	EM Hardening	11	Electronic Intelligence
4	EM Interference	12	Electronics Security
5	EM Intrusion	13	Electronic Reprogramming
6	EM Jamming	14	Emission Control (EMCON)
7	EM Pulse	15	Spectrum Management
8	Electronic Masking		

Table 3. The Principle Activities of Electronic Warfare (After Joint Publication 3-51, I-5 to I-8)

EM Compatibility (EMC) is the ability of systems and devices to operate in the intended EM environment without causing an unacceptable level of degradation. EMC includes system design configurations and clear concepts and doctrines to ensure this ability.

EM Deception is intentional radiation, re-radiation, alteration, denial, suppression, or reflection of EM energy with the purpose of providing misleading information to the enemy or enemy EM-dependent systems.

EM Hardening is the activities performed to protect personnel, facilities, and systems by filtering, attenuating, bonding, and grounding against unintentional affects of EM radiation.

EM Intrusion is placing EM energy intentionally into EM transmission paths in order to deceive operators and create confusion.

EM Interference is any EM-related disturbance that interrupts, obstructs, degrades, and limits the effectiveness of electronics and electrical equipment. This interference can be intentional or unintentional.

EM Jamming is a deliberate radiation, re-radiation, or reflection of EM energy to reduce or prevent the enemy from effectively using the EM spectrum, thus degrading or neutralizing combat capability.

EM Pulse is a strong pulse, commonly due to a nuclear explosion, that produces damaging current and voltages to disable electronic and electrical devices.

Electronic Masking is done to protect the friendly radiation against hostile electronic warfare support and signals intelligence (SIGINT) activities. It is basically controlled radiation of EM energy of friendly frequencies.

Electronic Probing is the deliberate radiation to be introduced into a potential adversary's devices and systems. Doing so enables friendly forces to learn about the functions and capabilities of hostile devices and systems.

Electronic Reconnaissance is the detection, location, identification, and evaluation of EM radiation.

Electronics Intelligence (ELINT) is the intelligence gained from foreign non-communications EM radiations. Intelligence can be technical, geolocational, or both.

Electronics Security is the activity designed to deny unauthorized persons access to valuable information, resulting in protection of friendly systems from activities like interception or non-communications radiations.

Electronic Reprogramming is purposefully made alterations or modifications of EW and target sensitive systems to adopt the changes in equipment, tactics, and the EM

environment. These changes might be due to friendly or hostile activities. The desired result of electronic reprogramming is to sustain and to increase the effectiveness of EW and target sensitive systems and devices used in defensive or offensive weapons and intelligence collection systems.

Emission Control (EMCON) is the selective and controlled use of EM, acoustic, and other emitters to achieve optimum C2 capabilities. EMCON measures include limiting the detection by enemy sensors and mutual interference among friendly systems

Spectrum Management is planning, coordinating, and managing the EM spectrum. The objective is to create an EM environment in which friendly electronic systems can perform their functions without interference or confusion (Joint Publication 3-51, I-6-7).

4. EW Subdivisions

Electronic Warfare (EW) is a term that includes a number of different electronic technologies for intelligence gathering and interfering with enemy operations. Electronic Intelligence (ELINT), or eavesdropping, has been going on since the invention of the telephone and telegraph (Schroer 2003, 49). Electronic warfare has three subdivisions as presented in Figure 14; electronic attack (EA), electronic warfare support (ES), and electronic protection (EP).

a. Electronic Attack (EA)

Electronic attack is the subdivision of EW that involves the use of EM energy, EM pulses, directed energy weapons (DEW) – which include high-energy lasers (HEL), charged particle beams (CPB), neutral particle beams (NPB), and high power microwave (HPM) – and anti-radiation weapons (ARMs). EA targets facilities, equipment, and personnel in order to destroy, neutralize, or degrade. Jamming and electromagnetic deception are good examples of EA. On the other hand, lasers designed to disrupt and blind optical sensors, RF weapons, and particle weapons that use EM energy as the primary destructive system are also examples of EA (Joint Publication 3-51, I-2).

The old term *electronic countermeasure* (ECM) is now obsolete and EA should be used instead. EA can be considered a type of fire that can be non-destructive as

well as destructive. For instance, jamming and spoofing are types of EA that are non-destructive, sometimes called ‘soft kill’. The use of anti-radiation missiles (ARMs) and directed energy weapons (DEW) are types of EA that are destructive, or ‘hard kill’. EA plays a significant role in almost all operations directed to C2 (Joint Publication 3-13, II-6).

Some other examples of EA are chaff, noise jamming, false targets, angle deception, and decoys. Chaff is one of the simplest and most widely used countermeasures. Originally chaff was composed of strips of metal foil but now consists of metal-coated dielectric fibers, thousands of which are stored in a small space.

Noise jamming, similar to thermal noise, increases the level of background noise to make the target returns undetectable (Stimson 1998, 439–440). A false target creates false target returns and thus confuses the operator and makes him unable to identify the real target return. Transponders and repeaters are used to create false returns (Stimson 1998, 446). Angle deception introduces angle-tracking errors in an enemy’s fire control radar or radar-guided missile which make the enemy missile miss its target. Cross-eye and terrain bounce jamming are techniques to accomplish angle deception (Stimson 1998, 450). Radar decoys are employed to confuse an enemy and draw the radar or the seeker of a radar-guided missile away from the deploying aircraft. Some types of decoys are expendable and towed (Stimson 1998, 453).

EA capabilities will grow along with the growth of radar capabilities. EA is becoming more sophisticated. The developments indicate that RF coverage and the responsiveness of noise jammers will increase and their escort and stand-off effectiveness will increase as well. Deception EA will advance and false targets will become more deceptive; they will become capable of showing realistic flight profiles of aircraft. EA systems will become more intelligent and responsive. They will adapt to the changes in the environment, like changes in radar characteristics and even waveforms (Stimson 1998, 454).

b. Electronic Protection (EP)

Replacing the old terminology of *electronic counter countermeasure* (ECCM), electronic protection (EP) is “active and passive means taken to protect

personnel, facilities, and equipment from any effects of friendly and enemy employment of EW that degrade, neutralize, or destroy friendly combat capability" (Joint Publication 3-51, I-2).

Examples are electronic masking, goggles filtering out harmful wavelengths of laser light, EW reprogramming, frequency deconfliction, and protection from friendly and enemy EW. Some advanced EP techniques are sidelobe cancellation, mainlobe jamming cancellation, vastly increased RF bandwidths, sensor fusion, offensive EP, and application of artificial intelligence (AI) to EP development.

c. Electronic Warfare Support (ES)

ES includes actions to search for, intercept, and identify enemy use of the EM spectrum. It also locates and localizes EM radiation, both intentional as well as unintentional.

The primary purpose of ES during these activities is immediate threat recognition, targeting, planning, and conducting future operations. The information required for conducting other EW operations, targeting, and homing is provided by this subdivision. This data can also be used to produce signals intelligence (SIGINT), measurement and signature intelligence (MASINT), and battle damage assessment (BDA) (Joint Publication 3-51 I-2). MASINT is technically derived intelligence that detects, locates tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. Measurement and signature intelligence capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, radio frequency, spectroradiometric, and seismic sensing systems as well as gas, liquid, and solid materials sampling and analysis (Joint Publication 1-02, 328)

Laser warning receivers (LWR) that are used to detect and analyze a laser signal, threat warning, collection systems and direction finding systems (DF) are examples of electronic warfare support. ES is the term that replaced electronic support measures (ESM).

Threat warning is technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. Direction finding is a procedure for obtaining bearings of radio frequency

emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment (Joint Publication 1-02, 160).

As technology advances there are always new techniques and tactics introduced into EW. Under any circumstances, it is vital that all three subdivisions of EW be coordinated, integrated and synchronized for the achievement of the military campaign objective. Even though they may seem to be separate disciplines, one must understand all three subdivisions to be able to understand the EW ‘umbrella’. EW is not only a theoretical area of study; many real world applications reside within it.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. HISTORICAL PERSPECTIVES OF EW AND THE EVOLUTION OF IO

A. HISTORICAL PERSPECTIVE OF EW

> Superior weapons and superior tactics have always conferred advantage in war; the development of measure and countermeasure is a major thread running through the history of human conflict, and Man's use of electricity, electronics and the electromagnetic spectrum in war has been no exception…evolution of electronic warfare from the American Civil War to the present day…shows that many of the basic principles of what we now call 'Electronic Warfare' are far from new. (Browne and Thurbon 1998, 3)

The history of Electronic Warfare does not actually begin with the Second World War as most people think. In fact, the roots of Electronic Warfare history can even be found in the U.S. Civil War in 1861. Until the large scale use of the telegraph, invented in 1837 by Samuel F.B. Morse, the primary communication means between the Navy Department in Washington, D.C., and the U.S. Navy Pacific Squadron was a *dispatch vessel*. But "speaking wires" spread so quickly that in 1858 a trans-Atlantic link was established, and the use of telegraph cables over the land became commonplace. With the outbreak of the Civil War in 1861, telegraph wires became one of the most important targets for cavalry. Union forces were more vulnerable to these cavalry raids than the Confederation forces, because the Union forces used the telegraph extensively (see Figure 15). Cavalry men switched military telegraph traffic to the wrong destinations, transmitted false orders to Union commanders, and also cut the wires to deny the information to the Union forces (Price 1984, 1–2).

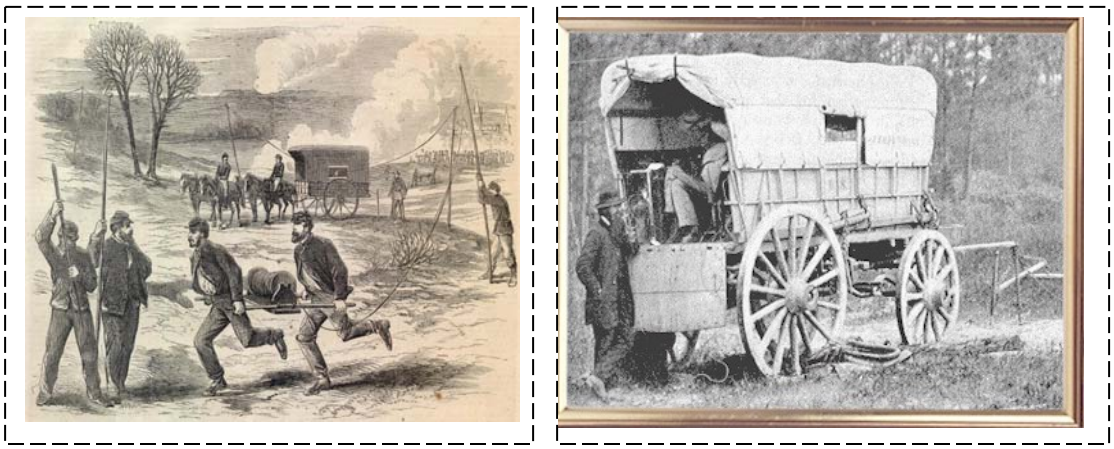


Figure 15. Telegraph Activities During US Civil War (left) and Telegraph Wagon (right) (1864) (From Civil War Homepage 2006)

Military commanders were able to establish fast and accurate communications over long distances with the telegraph, making its use attractive to both sides of the conflict. These can be considered as early applications of Command, Control, Communications, and Intelligence (C3I). The cavalry of both sides were trying to disrupt the other side's ability to employ effective C3I. These tactics are early examples of signals intelligence, jamming, and deception (Browne and Thurbon 1998, 3). Although the telegraph can not be considered a part of electronic warfare because it does not radiate electromagnetic energy, it is important to understand these early counter-C3I tactics as they relate to modern EW techniques, albeit in different forms.

1. Before and During the First World War

In 1888, German Heinrich Hertz demonstrated that "…electrical sparks would propagate signals into the space." This demonstration stimulated interest in Hertzian waves and led to the development of a radio system in England which was able to transmit Morse signals over 100 yards in 1895. Within two years, Italian Guglielma Marconi sent and received signals over two miles. With the increased range, radio communications became suitable for marine communications. In 1899 Marconi radio sets increased the transmission range to 89 miles (Price 1984, 1–3).

It was not long until the denial of this capability was achieved, spawning what we now think of as Electronic Warfare (EW). The first known instance of deliberate

jamming was surprisingly not for military, but for civilian purposes during America's Cup yacht races in 1901 in the United States.

> The first recorded instance of deliberate radio jamming took place in September 1901, in the U.S. Interestingly, it was aimed at securing commercial gain rather than military advantage. As now, there was considerable public interest in the America's Cup yacht races, and the newspaper first to reach the stands carrying each result stood to reap a large profit. In that year, Marconi obtained a contract from Associated Press...Another company,…Wireless Telegraph Company of America, secured a contract…A third company, the American Wireless Telephone and Telegraph Co., …failed to get a sponsor but decided to exploit the situation (and)…used a transmitter more powerful than its competitors, and one of its engineers, John Pickard, worked out a method which allowed him to jam signals from the other companies while at the same time reporting on the progress of the race from his boat…thus only AWT & T was able to pass accurate reports on the races (Price 1984, 3).

Soon thereafter, the first intentional use of radio jamming by the military took place in 1902 during British Navy Fleet exercises in the Mediterranean. This was followed in 1903 during U.S. Navy Fleet maneuvers. The exercise group was divided into two squadrons, White and Blue. Both sides carried radios. As part of the exercise, the Blue Squadron was directed to use radio communications for enemy sighting reports and maneuvers, while the White Squadron was directed to attempt jamming of this use. Due to the interference of an officer who didn't understand the speed of transmission and reception, and who wanted to listen to the entire Blue transmission rather than interfere with it, jamming of the Blue Squadron signals was not attempted until transmission of the critical message was completed, negating its impact. The White Squadron was intercepted and soundly defeated by the Blue (Price 1984, 4). This is the first recorded instance of a conflict between two opposing interests which still exists today; those who want to listen to the enemy radio signals for intelligence and those who want to jam them to deny information to the enemy.

In the Russo-Japanese War (1904–1905), radio jamming was used purposefully to gain tactical advantage. This was the first war in which both sides used radio. While Japanese cruisers bombarded Port Arthur, smaller ships equipped with radio observed the fall of rounds and passed corrections. A Russian operator on the shore heard these

Japanese signals and used his spark transmitter to jam them. Therefore, the Russian damage and casualties were lower than expected.

Figure 16. A First World War Mobile Royal Navy Direction Finding (DF) Station (From Browne and Thurbon 1998, 6)

From 1905 to 1914 there were significant improvements in Wireless Telegraphy (WT) systems:

- Transmission ranges were improved.
- Bandwidths were reduced to accommodate more channels
- The number of available channels improved.
- Mutual interference was reduced
- There were advances in transmitter and receiver technology with improved reception
- Size and weight of WT sets were reduced to fit aircraft, which was a milestone in air-ground communications (Browne and Thurbon 1998, 4).

Means to exploit the EM environment continued to be developed. "In 1906, the U.S. Navy installed a primitive direction finder (DF) on the coal ship Lebanon for tests,

but it demonstrated limited capability" (Price 1984, 5). By the beginning of World War I, radio jamming was widely used by many nations. In the early months of 1915, the Royal Navy began to establish a chain of DF stations along the east coast of England as shown in Figure 16. The purpose was to locate ships or aircrafts by the bearings of these stations (Price 1984, 6).

Air-ground communication using radio during World War I was very important for reconnaissance and artillery spotting purposes. Although there was little deliberate jamming, most of jamming resulted from too many friendly aircraft flying very closely (Schroer 2003, 49).

Up to this point, the importance of encrypting a message was not fully understood. The Germans demonstrated this importance with their victory at Tannenberg over the Russians. The communications between Russian headquarters were unencrypted and the Germans were able to intercept and read them. Despite this realization of the importance of encryption, the Germans were unable to appreciate the vulnerability of their own codes and ciphers (Browne and Thurbon 1998, 5). Close to the end of WWI, the German U-boat Fleet became an important threat to Allied shipping and was a main target for Allied wireless intelligence. However it was not easy to track German submarines. After the U.S. Navy installed a ship-borne wireless DF capability for use in anti-submarine warfare, the Allied wireless intelligence service was able to track almost all German submarines in the North Sea, the Mediterranean, and the North Atlantic, even though they kept communications traffic to a minimum. In fact, Allied forces were helped by the German Naval Command who then thought that their codes and ciphers were unbreakable, and who underestimated the capabilities of Allied forces (Browne and Thurbon 1998, 7).

Table 4 shows the important events that took place before and during WWI, including technological developments that led the way for electronic warfare.

DATE	EVENT
1837	Samuel F.B. Morse invents telegraph
1858	The U.S. and Britain establish a trans-Atlantic undersea cable for communication.
1861	During the U.S. Civil War, the telegraph becomes an important target for enemy cavalry.
Early 1870	James Clark Maxwell's theory established the basis of propagation of electromagnetic waves in free space.
1888	German Heinrich Hertz demonstrated electrical sparks propagating signals into space.
1895	Captain H. Jackson's radio system transmits Morse signal over 100 yards in England.
1897	Italian Guglielma Marconi sends and receives signals over two miles.
1899	Marconi radio sets are able to pick up signals from 89 miles.
1901	The first recorded instance of deliberate radio jamming takes place in the U.S.
1902	The first intentional radio jamming for military purpose takes place in the Mediterranean.
1904–1905	During the Russo-Japanese War, radio jamming is used purposefully for tactical gain.
1906	The U.S. Navy installed a primitive direction finder on the coal ship Lebanon for tests.
1914–1915	There is a wide use of radio jamming; The Royal Navy establishes a chain of direction finding (DF) stations.
1917	The U.S. Navy installs a ship-borne wireless DF capability to conduct anti-submarine warfare.

Table 4. Important Events Relating to Electronic Warfare through World War I

2. 1919 to the End of Second World War

The period between the world wars included significant developments in electronic engineering. As a result of these developments, radio navigation aids and radar became great tools and played major roles in WWII. These two technologies also brought great complexity into the electronic warfare world and increased the amount of effort that was dedicated to conducting electronic warfare (Browne and Thurbon 1998, 10). The significant developments that made way for radar to play a major role in World War II are as follows:

- The performance and reliability of equipment was improved.
- The reception and transmission of higher frequencies became possible.
- RT systems became smaller and lighter.
- RT systems became available for short-range communications.
- Knowledge of the use of the electromagnetic spectrum expanded.

After World War I, a great effort was made by the U.S. Naval Research Laboratory (NRL) to improve communication between ships, aircraft, and ground stations. In 1926, NRL focused their efforts on avoiding enemy detection and detecting enemy transmissions and creating interference for the enemy.

In the early 1930s came the initial development of Radio Detection and Ranging (RADAR). Powerful transmitters, sensitive receivers, and sufficient antenna directionality enabled the development of RADAR (Price 1984, 7). NRL developed an "interference detector" as early as 1922 and was able to detect signals up to 50 miles away by 1934. During this period, Great Britain and Germany were also developing their own similar capabilities. In 1935, the British detected an aircraft at 17 miles with pulsed radar operating at 11 MHz, and in 1936 they extended the range to 75 miles. On the other hand, German radars operating at 600 MHz detected an aircraft from 12 miles away. The U.S., of course, did not lag behind, and a 200 MHz XAF radar detected an aircraft at 100 miles and ships at 15 miles, limited by the curvature of the Earth and the antenna height of the radar.

After these significant developments in the radar world, experts began to think about whether the location of the transmitter could be denied or defeated. This led to the first airborne jamming test which took place in London, where an interrupted, continuous wave transmitter was used. Immediately after this test, anti-jamming systems were integrated into the Chain Home radar systems along the coast of England, shown in Figure 17. The Chain Home was Great Britain's first operational air defense radar system. These anti-jamming systems were the first examples of electronic counter counter-measures (ECCM) (Price 1984, 9–10). In 1939, just before the outbreak of World War II, the first instance of airborne electronic intelligence (ELINT) occurred. An ELINT

mission was being carried out by the German airship Graf Zeppelin as it was cruising along the east coast of Great Britain. It was intercepting, recording, and assessing the radiation potential threat to the Luftwaffe that was coming from tall towers, the Chain Home radar system. Meanwhile, many experiments and developments took place in the U.S. Prior to entering World War II, the U.S. possessed radars, high frequency direction finding (HFDF) systems, and anti-jamming devices.

Figure 17. The Chain Home Low Station at Hopton on the Norfolk Coast (From Browne and Thurbon 1998, 14)

1940 was the year of the 'Battle of Beams' for Germany and the United Kingdom (UK). Using radio navigation systems, one of which was called Knickebein, the Germans acquired an accurate night bombing capability over ranges up to 200 nautical miles (NM). This was a development originally generated using the German Lorenz

Company's "blind approach" navigation system. As seen in Figure 18, two transmitted beams were arranged so that one transmits dots and the other transmits dashes. As a result the overlapping beams created a center line of continuous notes and following this note, pilots were able to navigate accurately in the dark of night. In early 1940, the UK was unaware of this German navigation system. Through the gathering of isolated small pieces of intelligence and limited use of the German Knickebein system, the British gained knowledge about how the Germans were able to navigate to London in the dark. The British modified their systems and employed jamming to defeat the Lorenz Beams, which eventually undermined German confidence in their night navigation system.

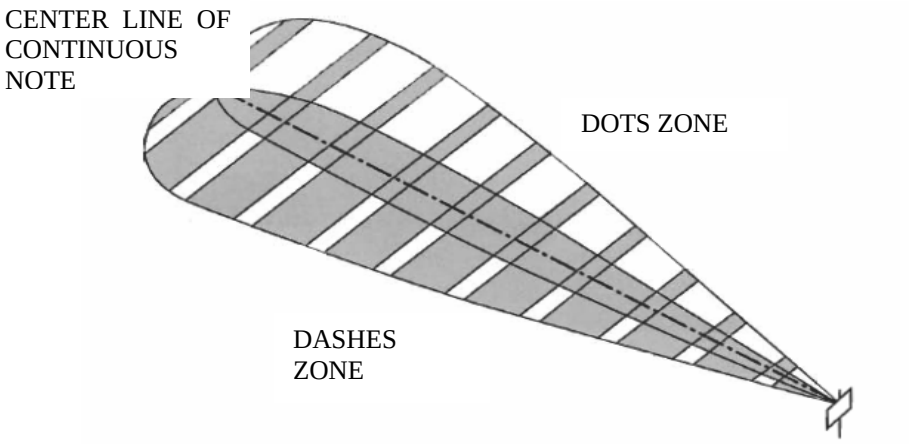


Figure 18. Arrangement of Beams in Lorenz Blind Approach System (From Browne and Thurbon 1998, 10)

Later, the British-developed "Y" radio monitoring stations and put counter-measures into them. Had the German Lorenz system not been recognized early and appropriate measures not been taken rapidly, the British could have been in a disastrous position due to German night bombardment ability.

The British developed a new EW system, the *Mandrel*. This was an airborne radar noise jammer. It was used to counter *Freya* radars by radiating signals to swamp the normal return echo, thereby obliterating formation size and range information. Freya radars were early warning radars that were being used by Germany to intercept and target British during German night bombardment Signals intercept by Mandrel and

photographic reconnaissance revealed the secrets of the Freya radar sites. Following 1944, programs in the U.S., Great Britain, Germany, Japan, and the Soviet Union gave fruit and radars were being installed on aircraft on a large scale. Meanwhile, the Germans increased the frequency range of Freya radars and reduced its jamming susceptibility by spreading its power in order to degrade the effectiveness of *Mandrel.*

At this point, a new kind of counter-measure against radar came into play: chaff, or "window" as the British called it (the German's referred to it as "duppel"). Chaff is basically a half-wave dipole which creates a strong radar return and echo that helps the target conceal itself from the radar. After some debate over using it, chaff was deployed, used, and proved effective against German radars (Browne and Thurbon 1998, 12–19). Chaff was sized to cover a range of frequencies and released in bundles. When the bundles opened in the air, they dispersed wide and large to produce false target echoes. The dispersion of the chaff depended upon altitude, weather, wind direction, and speed. EW became a cat-and-mouse game as the pendulum swung from EP to EA and back to EA (Schroer 2003, 51). It was a constant game of measures, counter-measures, and counter-counter measures.

There were also some applications of EW in the Pacific after the war in Europe was over, but there were no major EW technology developments. Immediately after World War II, development of U.S. electronic attack went dormant as other electronics developed. When the Soviet threat was recognized, the first priority became electronic intelligence (ELINT) activities to monitor Soviet radar deployment (Schroer 2003, 52).

3. 1946 to the First Gulf War

The most significant advances in electronic warfare that carry it to the modern day occurred particularly after the Second World War. However, if not for the inventions and development prior to and during Second World War, these significant advances could never have been realized.

Many of the advances in tactics and technology occurred during the Vietnam War; air tactics began to change in order to better benefit and counter electronic warfare capabilities. Electronic warfare officers (EWOs) or "Crows" played a major role in this conceptual change in air tactics during the Vietnam War. An interview about the Wild

Weasels with a current member of the Naval Postgraduate School (NPS) faculty who served as a USAF EWO is located in Appendix B.

a. EW during the Korean War (1950–1953) and U-2 Missions

During the Korean War, under the command of General MacArthur, the U.S. deployed 100 B-29 Superfortress heavy bomber aircraft to the theater. The North Korean Air Force had no effective means to counter the B-29 during the first five months of the war. This changed when the Chinese forces joined North Korea and the transonic MiG-15 jet fighter deployed to airfields in nearby Manchuria. The MiG-15 made life hazardous for bombers, restricting them to operate solely at night. The North Koreans also installed early-warning radars and radar-controlled anti-aircraft-artillery (AAA). Although countermeasures existed, the B-29s were not allowed to use chaff against the enemy radars or to jam the fighter communications frequencies because this would reveal U.S. EW capabilities that were reserved for the potential of a conflict with the Soviet Union. Only spot jamming of the AAA fire control radars was allowed. Consequently, aircraft losses became unacceptable. By October 1951, it was clear that darkness by itself was not a good cover and the restrictions on the use of chaff and the jamming of fighter control channels had to be abolished (Browne and Thurbon 1998, 26). Not applying the lessons learned from the Second World War demonstrated the harsh reality and critical nature of the EW mission in air warfare.

After this lesson, the USAF Strategic Air Command rebuilt the EW capability of its aircraft and EW crew members began to be considered as part of operational requirements, with simulators built to train the crew in electronic warfare.

Continuing into the early 1950s, the first operational surface-to-air missile (SAM) system, the SA-1 Guild, was built and deployed around Moscow. The more capable SA-2 Guideline quickly replaced the old SA-1 system. The SA-2 uses a Fan Song track-while-scan (TWS) radar to command-guided a missile; that is, guides its missile to the target by command signals from a ground controller system. The SA-2 Launcher and radar set is displayed in Figure 19. These Russian advancements stimulated the West and led to the development of various technologies critical to EW, such as transistors, traveling wave tubes (TWT), and spiral antennas. The development of airborne EW systems reduced the effectiveness of ground-based air defenses, requiring

more power, more complex jammer suites, and more money. More modern and capable aircraft were being used for Electronic Intelligence (ELINT) missions. The largest U.S. ELINT aircraft of the period was the Convair RB-36, which was equipped with a comprehensive EW suite.

Figure 19. SA-2 Guideline SAM and Its Radar Set (From Military Analysis Network (a) 2006)

By the early 1950s, the U.S. intelligence community needed images of Soviet radars. These images would be used for evasion and targeting purposes. The only method available to gain these images was by flying low over the targets and taking pictures of the radar sites. This action risked Soviet retaliation and was banned by

President Truman. Instead, three USAF RB-45Cs were painted with Royal Air Force (RAF) markings and performed the mission. The use of aircraft for such missions led to the development of the U-2.

The U-2 was designed for electronic intelligence (ELINT) and reconnaissance purposes. Information such as the frequency and detailed circuitry of an emitter are important to employ effective electronic protection (EP) as well as to conduct electronic attack (EA). U-2s not only photographed military and industrial installations but also collected signals intelligence (SIGINT) on operating radars.

The intelligence collected by U-2s was very valuable because it could help determine characteristics of the enemy emitters and even defense system structure. The following intelligence was typically collected by U-2s:

- The frequency of the enemy emitter. Intelligence officers can deduct how accurate targets can be plotted, how well can it see through the rain and cloud.
- The rate at which a radar beam can be made to scan through an aircraft. It is possible to deduce the purpose of radar; 360 degrees search radar, height finder, locking radar, or missile control radar
- The rate at which the radar pulses are transmitted. The maximum usable range of radar can be determined.
- Time width of the radar pulses. The resolution or discrimination ability among many aircraft flying together can be learned.
- Signals that are picked up. The location of the emitter can be calculated. This can relate to the area where defense is strong backed up by many types of radar (Price 1977, 256).

After a few successful flights, a U-2B was shot down, leading to a U.S. government ban of U-2 overflight of the Soviet Union. It became clear that high altitude on its own did not provide enough protection from long-range SAM systems (Browne and Thurbon 1998, 27–28). There were four possible ways of increasing the probability of survival for a manned aircraft under these circumstances:

- Fly even higher and faster and use EW systems to degrade the performance of defensive systems.
- Fly even higher and faster and use stand-off weapons to stay clear of the lethal range in most heavily defended areas.
- Fly so low and so fast that ground clutter and terrain masking reduced radar effectiveness.
- Fly so low and so fast that exposure times were short enough to make effective engagements unlikely.

The first new U.S. strategic reconnaissance aircraft developed following the shoot-down and guideline establishment was the SR-71, and the B-52, B-58, and RAF V-Bombers were modified or developed with these guidelines in mind. In the late 1950s, the Quail radar decoy missile was introduced. Launched from a B-52, it gave the appearance of a small aircraft. To complement the illusion, it could carry and employ jamming transmitters to simulate a bomber (Price 1977, 254). The development of EW was stimulated by the military competition between the U.S. and the Soviet Union, and served a role in maintaining a critical balance of mutual deterrence (Browne and Thurbon 1998, 30).

During the late 1950s, space came into play in the EW world. The US *Moonbounce* program collected radiation from Soviet radars after it was reflected from the surface of the moon and back to the Earth. A number of these observations were able to provide useful intelligence to the U.S., unknown by the Soviet Union.

b. EW during the Vietnam War (1957–1953)

The U.S. did not initially intend to fight the war in Vietnam itself, but rather intended to provide military assistance to the South Vietnamese to defend themselves. With the deterioration of the South Vietnamese military and political situation, U.S. support and involvement in operations increased to the point that the U.S. conducted most of the fighting. During this entire period, air operations were firmly controlled by the U.S. military.

The U.S. wanted to keep the Soviet Union and China out of the conflict and at the same time to reduce any adverse public opinion. The cost of these political decisions was high; between 1964 and 1973, 4,700 aircraft were shot down by fighters, AAA, small arms fire, and SAMs. This was partly due to the fact that limitations and restrictions were placed on air operations, reducing their effectiveness and placing the crews at greater risk.

Aircraft from the USS Coral Sea detected the first SA-2s sighted in Vietnam. This SAM was infamous for shooting down two U-2s. It was designed to take down high-flying U-2 and V-Bomber threats. The SA-2 had a range of about 20 NM and a ceiling of approximately 80,000 feet. The introduction of the SA-2 to Vietnam forced the U.S. to change tactics; aircraft were forced down to low altitudes where they were within the range of AAA. The losses to AAA and ground fire began to mount, necessitating a solution. The North Vietnamese deployed around 200 early-warning and ground-controlled interception (GCI) radars, and around 2,000 AAA.

This solution to SAMs was partly found with the development of the Wild Weasel mission (Browne and Thurbon 1998, 30). The first Radar Homing and Warning (RHAW) system, the AN/APR-25, was developed in 1965 and was used to equip the F-100F 'Wild Weasel' aircraft. This RHAW system not only detected radar emissions, but also displayed the relative bearing of the emitter and gave warning to the crew if the aircraft was being tracked by threat radars.

With this equipment, the USAF developed the tactics that would mark these special crews as Wild Weasels. They were special units comprised of fighter-bomber aircraft and crews that engaged the enemy radar-guided surface-to-air missile and gun batteries. These units provided cover to other fighter-bombers attacking conventional targets. As the state of the technology progressed, the Wild Weasels were armed with Shrike and Standard anti-radiation missiles (ARM) which homed in on the signals from the enemy radar (Price 1977, 265) (see Figure 21).

> Four two-seat North American F-100Fs were fitted with suites comprising RHAW, radar signal analysis and missile launch warning receiver systems, manned by experienced F-100 pilots and Electronic Warfare Officers (EWO, or Crows) from SAC's B-52 fleet, and flown

> on missions over North Vietnam from the beginning of December 1965. They flew ahead of the attack aircraft to tempt SA-2 sites into revealing themselves and attacked those that did with rockets, napalm, cannon, and from March 1966, with Texas instruments AGM-45 *Shrike* Anti-Radiation Missiles (ARM). The F-100Fs destroyed a number of SA-2 sites over the next six months, kept many more closed down during critical phases of attacks, and developed the basic Wild Weasel tactics before they were replaced from May 1966 by similarly equipped, but faster, two-seat Republic F-105Fs. Subsequent improvements to the electronics and weapons, including the introduction of General Dynamics AGM-78 Standard ARM which weighed over 1,350 lbs and had a range of some 13.5 NM, produced the F-105G which began to replace F-105Fs from April 1968 (Browne and Thurbon 1998, 33).

Along with the development of the Wild Weasels, the U.S. also introduced the first tactical jamming pods to be fitted on fighter-bomber aircraft. These new technologies, such as the Quick Reaction Capability (QRC)-160 pods, and later the AN/ALQ-87 family of communication and radar jamming pods, provided protection to tactical aircraft beginning in 1965.

Nearing the end of the war during Linebacker II, which was the second of a series of air operations with the order of "to win this war" over the Vietnam air defense, the internal EW suites provided self protection when bombing from high altitude. During the bombardment, F-105G Wild Weasels and General Dynamics F-111s attacked the North Vietnamese SAM sites and airfields while EB-66s provided stand-off jamming. Linebacker II was proof that "a powerful barrage of electronic jamming, combined with vast quantities of chaff and carefully evolved anti-missile tactics backed by Wild Weasel attacks on the launching sites could reduce the effectiveness of the air defense system (ADS) (Price 1977, 271). The loss rate was significantly reduced by the coordination of effective tactics with electronic warfare techniques. There are many more lessons learned from the Vietnam War than can not be presented here, but some of them are:

- Effective EW capability is crucial for air operations and aircraft survivability in a well-integrated and effective enemy air defense environment. Wild Weasel aircraft, RHAW systems and jamming pods provided the proof of this assertion.

- Combining airborne surveillance and control, air defense, attack, EW, and reconnaissance aircraft in tightly coordinated strike packages was essential to attacks on heavily defended targets in Vietnam.
- It was a clear message to the world that proliferation of airborne EW systems, realistic EW training, and an escalating air defense threat was gaining importance in battles (Browne and Thurbon 1998, 34).

c. Yom Kippur (1973) and the Bekaa Valley (1982)

In October 1973, Syria and Egypt launched a massive attack against Israel to regain the territory they lost in the 1967 Six Day War. The Israeli pilots were familiar with the SA-2 and SA-3 systems, which were effective against high-flying aircraft, but they had little knowledge of the SA-6 system deployed by the Soviets. This SAM employed semi-active radar homing and was more accurate and jam resistant than previous SAM systems. Mounting fire control radars and missile launchers on tracked vehicles gave the system excellent mobility. Because the SA-6 had not been previously exploited, and had its first operational use during this conflict, there had not been enough opportunity to properly prepare electronic warfare systems to deal with this new threat. Moreover, it was complemented by the ZSU 23-4 anti-aircraft gun system that targets low-flying aircrafts. Also deployed into the air defense system was the SA-7 IR-guided MANPAD SAM. SA-6 and SA-7 MANPADs can be seen in Figure 20. The SA-7 was a small man-portable heat-seeking anti-aircraft missile that was effective against helicopters and slower low-flying aircraft. Facing these new threats, the Israelis initially suffered heavy losses, with more than eighty Israeli aircraft destroyed during the first week of the war and many more damaged (Price 1977, 273). This shows the importance of deploying new equipment that can surprise an enemy having no knowledge or measures to counter a new threat.

Having painfully learned from this experience, Israel invested heavily in C^3I and EW systems; airborne, rocket and artillery propelled defense suppression weapons; intelligence gathering; planning; and training. These investments benefited Israel during their 1982 conflict with Syria. Israel's plan for the invasion of south Lebanon started with attacks by aircraft on Palestine Liberation Organization bases on June 4th, and continued with a ground force advance up the coastal plain towards Beirut

on the 6th. The Syrian Air Force tried to disrupt the Israeli ground and air attacks but was ineffective. Israel launched a well-planned and pre-rehearsed attack against Bekaa Valley where the strongest Syrian air defense system resided.

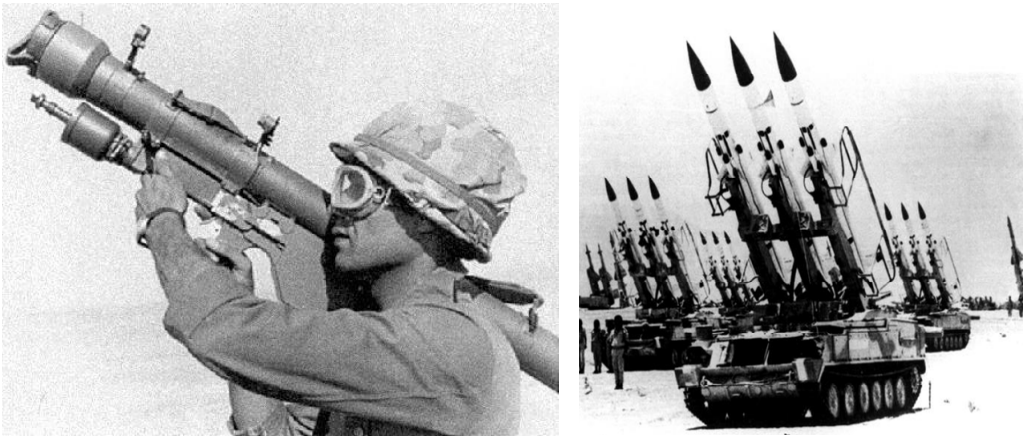


Figure 20. SA-7 MANPAD (left) and SA-6 (right) (From Military Analysis Network (d) 2006)

The Syrians had not moved any of the SA-6 Gainful systems for over a year. Because of this error, Israel had learned the exact location of many of the elements of the SAM, radar, and communications infrastructure as well as their electronic fingerprints. Simulating the real attack profiles and radar signatures, remote piloted vehicles (RPV) flew on June 9th and fooled the Syrians into launches from their SAM sites. After the Syrians had reloaded their weapons, Israeli long-range artillery and rocket systems shelled these SAM sites, and soon after, aircraft came into play and launched AGM-45 Shrikes, AGM-78 Standard-ARMs, and AGM-65 Mavericks against the early warning and fire control radars. Pictures of these missiles can be seen in Figure 21. At the same time, the Israeli Air Force successfully employed jamming and chaff, denying the Syrian radar operators a picture of the air operation's second wave, which destroyed many of the remaining air defense system elements. In only half an hour on June 9th, 19 SA-6 sites were destroyed, the GCI system was heavily damaged, and air-to-ground and air-to-air communications were continuously being jammed (Browne and Thurbon 1998, 35–36).

AGM-78 Standard ARM

AGM-45 Shrike ARM

AGM-65 Maverick

Figure 21. Different Types of missiles Used During Arab-Israel Conflicts (From Military Analysis Network (d). 2006)

d. The First Gulf War (Operation DESERT STORM)

> Electronic Warfare has been a necessary and oft-times effective component of air war since World War II. But in Desert Storm, only the stealth fighter ventured into enemy airspace unaccompanied by a swarm of supporting airplanes: some launching decoys to trigger enemy radar into action; some carrying anti-radiation missiles that instantly homed in as those radars came up. Stand-off jammers were out of range of enemy weapons but close enough to blank out enemy radios. It was a devastating combination of hard and soft kill, and it wrote a new chapter in the saga of warfare (Campen 1992, XIV).

In the First Gulf War the importance of surprise and well-planned air attacks prior to the conduct of ground operations again proved to be decisive in the overall campaign. The strategy was simple: build enough coalition forces so that they could contain an Iraqi attack, then reduce the Iraqi ground forces' effectiveness to fight by at least fifty percent through large-scale air attacks, and finally attack them with ground and air forces simultaneously (Browne and Thurbon 1998, 37).

The Iraqi air defense system had 17,000 SAMs and 10,000 AAA and a wide variety of complex communications links (Watson 1993, 158). The Iraqi Air Force

had 550 aircraft, of which a mix of obsolete Soviet Tu-16 and Tu-22 medium bombers, more modern Su-25 Frogfoot, a core of MiG-21, and a few long-range Su-24 fighter-bombers fulfilled the ground attack role. For air defense the Iraqis used the MiG-23, MIG-25, and the MiG-29 aircraft. Iraq's complex ground-air-defense system consisted of SA-2, SA-3, SA-6, SA-8, and Roland missile batteries, supplemented by hand-held missile launchers (SA-7), and long- and short-range radar screening the border of Iraq and the city of Baghdad, where all communications were centered. Table 5 summarizes some of the assets that were used during the First Gulf War by the Coalition forces (Watson 1993, 157–163).

	PLATFORM	**MISSION**
SUPPORT	USAF RC-135	Extensive SIGINT (ELINT/COMINT) picture
	USAF U-2R	Collection of COMINT
	RAF Nimrod R.2	ES purposes
	French DC-8 Sarigue, EC-160 Gabriel, SA330 Puma Helicopter	ES purposes
	USAF EA-6B, F-4G Wild Weasel, EF-111A Tornado, B-52, Jaguar, F-16, F-111, F-117A Nighthawk, A-10	Refinement of the electronic order of battle (EOB), SEAD, hard-kill missions
	US Magnum and Vortex ELINT KH-12 imaging satellites	IMINT/ELINT purposes
ATTACK	USAF EF-111A US Marine and Navy EA-6B	Escort air strikes, provide jamming support to penetrate targets
	USAF EC-130H Compass Call	Communications jamming, spoofing capability
	RAF Tornado GR1	Hard-kill mission with ALARM ARM
	US Navy Tomahawk	Cruise missile (CM) for hard-kill missions

PROTECTION	Emission Control (EMCON)	Reduce the radiated energy that is vulnerable to hostile ES and EA
	US Army SINCGARS, USAF Have Quick radio	Had integral EP capabilities

Table 5. Assets Used For ES, EA and EP Purposes During the First Gulf War

For the Coalition forces, the U.S. provided squadrons of F-14D and F-15C interceptors, F-16, F-117A Stealth Fighters, B-52 strategic bombers, F-4G Wild Weasels armed with HARMs, A-10 Warthog tank killers, and Hellfire-capable Apache and Super Cobra helicopters for tactical ground support. Other main aircraft were French Jaguars and British GR-1 and F-3 Tornados. Conventional-warhead Tomahawk cruise missiles (CM) were also extensively used, launched from the battleships Missouri and Wisconsin, along with other naval platforms (Watson 1995, 161–162). The Tomahawk is a cruise missile equipped with a small camera. It matches the video to preloaded maps onboard, enabling the missile to cruise over the terrain using reference points.

For the first time, chips and computers played a significant role in warfare, delivering more information, intelligence, and fire power than ever seen before. A new kind of chaff developed by the U.S. was also deployed in the Gulf War. First tested in the Pacific Ocean near San Diego, this chaff, instead of falling harmlessly to sea as intended, was blown toward the land some 90 miles away and draped over electric power lines, shorting the transformers and causing blackouts in some parts of San Diego during its testing (Adams 1998, 37). Although Iraq's leadership, communication and transportation systems, nuclear biological and chemical (NBC) warfare capabilities, and infrastructure and power supply networks were targeted, the first priority was to disrupt its command and control system and achieve 'air superiority'.

Among the first priority targets were command posts, communication systems, airfields, air defense radars, operation centers, and the electrical generation and distribution networks (Browne and Thurbon 1998, 38). Similar to tactics used in the Bekaa Valley by Israel, the first breach was made against two radar stations near the border southwest of Baghdad by eight AH-64A attack helicopters, destroying them in two minutes. The air defense operations center in Nukheyb was destroyed by two F-117As with GBU-27 2,000 pound laser-guided bombs. Immediately after those attacks, command and communications targets and elements of the electrical power network were demolished by F-117As and R/UGM-109C/D Tomahawk Land Attack Missiles (TLAM C/Ds), without being detected by the Iraqi air defenses.

During the next wave, the Iraqis thought they shot down a number of aircraft, but their celebration was short-lived because they had been decoyed by BQM-74 drones and Tactical Air Launched Decoys (TALDs). BQM-74 was an unmanned jet-powered aircraft. Although it was only thirteen feet long, it could project the radar image of a much larger airplane. “Moments behind the drones and TALDs were a mass of seventy allied aircraft armed with radar-killing HARM (U.S.) and ALARM (British) missiles whose purpose was to find and attack the Iraqi radar beams, then follow the path of the beam back to the radar stations and destroy them” (Adams 1998, 45). It was relatively simple for the F-4Gs to accomplish this mission provided that all the radar systems and anti-aircraft batteries were operating in an attempt to find incoming targets, which in fact were the drones causing them to believe a real air strike was in progress. These first waves of conventional strike aircraft used tactics similar to those in Vietnam, where they were protected by fighter cover and EW support. They were able to fly in clean air corridors and strike targets in Iraq.

In the first Gulf War precision-guided munitions (PGMs) significantly increased the overall effectiveness of the air campaign, not only because of their accuracy and ability to destroy point targets, but also because of their relatively low percentage of collateral damage. The F-117A, which has a very low radar and infrared signature, was another contributing factor to the success of the air campaign. They were undetectable by the enemy radars. The loss rate for Coalition air forces was very low. This was partly due to the fact that the Coalition forces gathered accurate SIGINT on Iraqi air defense

systems, made great efforts to conduct defense suppression, utilized effective HARM and ALARM anti-radiation missiles, and employed well-developed EW systems in their aircraft, and well-trained crew to use these systems.

The ground war that followed the air strikes was supported by two E-8A JSTARS (Joint Surveillance and Target Attack Radar System), similar to the support that E-3 AWACS (Airborne Warning and Control System) gave air strikes. E-8 JSTARS prevented Iraqi ground forces from moving safely and undetected across the desert day and night. One picture that is provided by JSTARS of the Iraqi retreat from Kuwait is presented in Figure 22. In his book The Next World War, James Adams comments on the AWACS and JSTARS:

> Overreaching the whole campaign was the web of information gathering and transmission that was as vital as aviation kerosene itself. E-3 AWACS (Airborne Warning and Control System) aircraft, essentially a Boeing 707 on top of which a large mushroom-like structure had been fixed to house a mass of electronic surveillance equipment, patrolled the skies above the Iraqi border. The AWACS were able to view the entire airspace of conflict…E-8 JSTARS aircraft, another version of Boeing 707, provided the same function as AWACS on behalf of ground forces, their role being to detect enemy activity such as convoys, tank formations, and Scud missile sites that the Iraqis had hidden in remote places (Adams 1998, 45).

The AWACS acted as the eyes for the air forces, JSTARS did the same for the ground forces, and the RC-135s were the ears of the allied forces. The RC-135 aircraft monitored and eavesdropped on Iraqi communications, and located and localized the source of any hostile electronic emissions. This data was then passed to Tactical Air Control Centers (TACC), where the TACC planned and directed attacks against these locations (Adams 1998, 46).

Shortly after the ground war started, the Iraqis lost their will to fight. The ground war lasted just 100 hours with fewer than 500 Coalition casualties (Browne and Thurbon 1998, 39–40).

Figure 22. E-8 A JSTAR Moving Target Indication Picture of the Area of Kuwait City in Late February 1991. Each Dot Is A Vehicle or A Group Of Vehicles Heading North On The Roads As The Iraqi Forces Pulled Out Of Kuwait (From Browne And Thurbon 1998, 38)

The Defense Satellite Communications Systems (DSCS) satellites were used extensively to provide vital communications links, supplementing an insufficient wire and microwave structure on the ground. The Global Positioning System (GPS) was one of the more important contributions provided by space-based systems. GPS provided the data for soldiers in every echelon to determine their location when other systems were insufficient. Special Forces made use of GPS in northeastern Iraq for targeting and destroying ground forces as well as Scud missiles (Adams 1998, 48). Infrared technology also played a significant role in air campaigns. Aircraft losses due to infrared SAMs were almost equal to the total of all other counter-measures. This shows that SAMs are big threats for aircrafts. In addition, the total loss of US aircraft due to Infra-Red (IR) SAMs

was actually more than the total loss of AAA and RF SAMs. This indicates the importance of IR-guided systems during the combat.

The Gulf War was a real-life test of weapons, machines, and technology that had never been used in combat before. Many lessons related to the future of military operations may be drawn from Operation DESERT STORM. An obvious lesson is that the winner of the next major war will most likely control the electromagnetic spectrum and deploy small forces with greater combat power. The Gulf War initiated the use of *Information Warfare*, in which EW continues to play a major role.

B. THE BIRTH AND THE EVOLUTION OF INFORMATION OPERATIONS

1. Historical Perspectives of Information Operations

It is impossible to know what the first applications of what is now called information operations were, but some examples can be found in various studies. One of those sources is *The First Information Warfare Web Site*, which sets a timeline for IO that starts at 1200 BC with the Greeks' use of the Trojan horse to gain entrance to Troy (Military Deception). Another source is the interview of Wanja Eric Naef by Professor Dan Kuehl, where Professor Dan Kuehl depicts an Assyrian King from 600 BC on the mountain with the "heaped-up skulls from his enemies" (Psychological Operations). According to Professor Dan Kuehl, this was a primitive type of information operations because the Assyrian King was actually trying to influence the enemies by the display of skulls, intimidating them with the message, "Don't mess with Assyrians or you will lose your head." Professor Kuehl is right, as the ultimate aim of IO is to influence the adversary's decision-making processes in a manner favorable to friendly forces. This is exactly what the Assyrian King was trying to achieve.

Though the history of IO is significant, it is not important when the first use of IO took place. The bottom line, as demonstrated by the examples above, is that IO and IW, while not known by these terms, have been around for a long time. They have become increasingly popular because of the increases in the number and availability of tools that can be used to employ them. Especially during the last quarter of the 20th century, the technologies available for information systems and communications made it easier to conceptualize and conduct IO as a discipline, and therefore, have led to much research,

development, and discussion in this area. To many combat experts, Operation Desert Storm is considered the first information war.

2. The Evolution of the Term "Information Operations"

Although the effort to gain information superiority goes back to very early dates in history, the theory that information could actually play a significant and even decisive role in the way warfare is conducted was first introduced by Dr. Thomas P. Rona in 1976. In his report titled "Weapons Systems and Information War," Dr. Rona drew attention to the close and vital relationship between information and weapon effectiveness. Although he did not use the terms that are used today, he foresaw a system-of-systems, global grids, and network-centric warfare (NCW). The critical but ignored relationship between information systems and warfare platforms became clear in the Persian Gulf War in 1991 (Campen and Dearth 2000, 289). Most of the critical thinking about IO began in the early 1980s. Then, in Operation Desert Storm, Allied forces had information superiority and a modern weapons advantage over their adversary; therefore, they were able to end the war quickly and decisively. Despite the fact that the information infrastructure was not well-planned and organized as contained in theory, this conflict taught that understanding the relationship between information and weapon systems, and possessing this superiority over the enemy, could be a decisive factor in the cost and result of a war.

In 1992, the Office of the Secretary of Defense (OSD) published a classified document titled "Information Warfare." Three months later, the Joint Chief of Staff issued an unclassified Memorandum of Policy 30 (MOP 30) titled "Command and Control Warfare (C2W)" which was broader than the OSD document. Being limited in scope and not compatible with service doctrines, the term C2W was changed to information operations (IO) by the Army and the Air Force. They claimed that the employment of information was also useful in peacekeeping and crisis management, and even in war it was not limited to Command and Control (C2) systems.

In addition to these reasons, the Army and the Air Force also thought that information was a useful tool for federal, state, and local agencies (Campen and Dearth 2000, 292). This idea is important because policy makers must use the military and diplomatic or civilian instruments together to be successful in peacekeeping operations

and crisis management. These two instruments should not be considered as separate entities because they intersect each other at many points during the conduct of IO.

The critical relationship between information and weapon systems was strongly evident in examples such as the Gulf War, Bosnia, and Kosovo conflicts. Information Operations helped to shape the information space in all these conflicts. The ultimate goal of war is not to destroy everything, but to shape the behavior of the adversary in a favorable manner. Shaping the behavior of the enemy takes more than just managing the battlespace. We must also manage the information space. During wars in the past, like those in Kuwait and Kosovo, victory was attained in a conventional manner—Kuwait was freed and the Serbian army withdrew from Kosovo—but they did not secure the ultimate foreign policy objectives. The dictatorships in Iraq and Serbia remained in power after the termination of hostilities (Campen and Dearth 2000, 292). In order to conduct IO, all of these capabilities and activities, shown in Figure 23, must be integrated carefully.

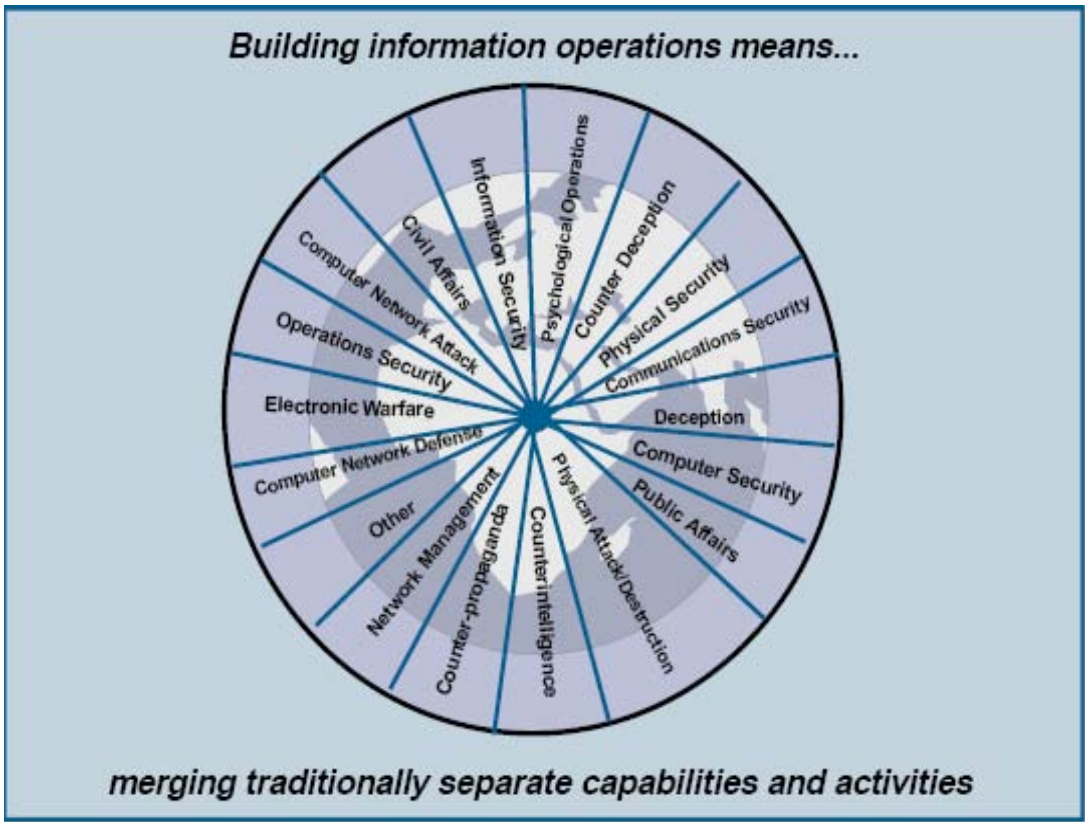


Figure 23. IO Capabilities and Related Activities (From Joint Publication 3-51, I-5)

3. Differences between C2W, IW and IO

According to Joint Publication 3-13, information operations (IO) are described as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own" (Joint Publication 3-13, I-1). IO supporting capabilities are information assurance (IA), physical security, physical attack, counter-intelligence (CI), and combat camera (COMCAM). IO related capabilities include public affairs (PA), civil military operations (CMO), and defense support to public diplomacy (DSPD) (See Table 6).

CORE COMPETENCIES	
Electronic Warfare	
Operations Security	
Military Deception	
Computer Network Operations	
Psychological Operations	
SUPOORTING COMPETENCIES	**RELATED COMPETENCIES**
Information Assurance	Public Affairs
Physical Security	Civil Military Operations
Physical Attack	Defense Support to Public Diplomacy
Counter-Intelligence	
Combat Camera	

Table 6. Information Operations Competencies

Information Warfare (IW) can be described as that part of information operations which is conducted during time of crisis or conflict to achieve specific objectives over an adversary. Although replaced by the terms IO and IW, Command and Control Warfare (C2W) is described in Joint Publication 3-13.1 as "the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions" (Joint Publication 3-13.1, V).

From one perspective, information warfare is a wartime, or conflict, subdivision of IO. Although already superseded by the terms IO and IW, C2W is an application of IW in military operations that targets the enemy and protects friendly command and control capabilities and assets. That is why it can be considered as a subset of IW. But actually, employed C2W elements might create effects outside the command and control target set. They also differ in terms of the elements they use to accomplish their aim. IO employs broader assets and methods when compared with IW and C2W. These differences are depicted in Table 7. IW contains six elements: CNA, Deception, Destruction, EW, Operations Security, and PSYOP, while IO is much more comprehensive than IW, including supporting and related elements (Armistead 2004, 19).

Questions / **Warfare**	**What kinds of Instruments are used?**	**When is it used?**	**Defensive or Offensive?**	**What is the Objective?**
Command & Control Warfare (C2W)	OPSEC, MILDEC, PSYOP, EW, Physical Destruction	Conflict Crisis	Offensive Defensive	To influence, degrade, or destroy adversary C2 capabilities To protect friendly C2 capabilities
Information Warfare (IW)	OPSEC, MILDEC, PSYOP, EW, Destruction, CNA	Conflict Crisis	Offensive Defensive	To achieve specific objectives over the enemy during wartime
Information Operations (IO)	OPSEC, MILDEC, PSYOP, EW, Physical Destruction, IA, Physical Security, CI, COMCAM, PA, CMO, DSPD	Conflict Crisis Peace	Offensive Defensive	To influence, disrupt, corrupt, or usurp adversarial human and automated decision making To protect friendly decision making

Table 7. Differences Between IO, IW, and C2W

The most important features that distinguish the line between information operations and information warfare are as follows:

- IO can be used to shape the pre-hostility environment so that conflict is possibly avoided.
- To many theorists, IW is what is done during the battle when pre-hostility IO fails.

- IO includes thirteen elements. IW contains six, and C2W contains only five.
- IO is a strategic campaign and much broader than IW. IO is conducted from peace to war and back to peace, as depicted in Figure 24.
- In IO, not only enemy but also friendly forces are studied (Armistead 2004, 20). The protection of friendly decision making process is as equally important as influencing the adversary's.

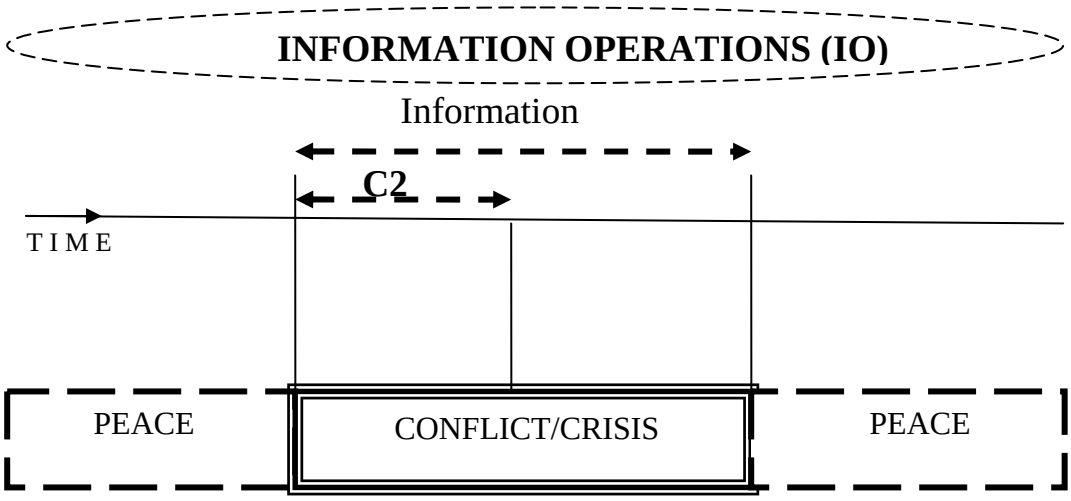


Figure 24. Spectrum of Conduct of IO, IW, and C2W

Even though they use different tools and are employed across a different time spectrum, the ultimate goal in all three kinds of warfare is achieving national objectives. The most important reason for the IO evolution from C2W and then from IW is the pursuit of the best means to accomplish this goal. Have the best tools to achieve the national objectives been discovered yet? Nobody knows for sure. What is certain is that people are always seeking the best tools to utilize, now and in the future, therefore IO should not be perceived as a solid, stable concept, instead it should be seen as an open ended, flexible tool which is ready to evolve and transform with future warfare requirements.

V. INTERACTION AND RELATIONSHIP BETWEEN EW AND EACH IO COMPETENCY

In this chapter, the interaction and relationship between electronic warfare, which is itself a core competency of information operations, and other IO core, supporting, and related competencies will be examined. Sometimes vague or indistinct, and sometimes direct or indirect, the relationship to electronic warfare is intrinsic due to the nature of IO. By definition information operations requires integration, coordination, and synchronization of core, related, and supporting competencies; therefore, the mutual relationship between the competencies is inevitable. As a matter of fact, the more communications and computing systems technologies rely on the use of the electromagnetic spectrum in the collection, storage, processing, and dissemination of information, the greater the interaction is of EW with the other competencies of IO. This shows the essential nature of the role that EW plays in IO.

A. ELECTRONIC WARFARE INTERACTION WITH CORE COMPETENCIES

As we know, PSYOP, OPSEC, and MILDEC have played significant roles during the course of military history. But in the last century, and particularly in the second half, EW has joined with those capabilities and become one of the major competencies of warfare. This has been followed in recent years by the emergence of computer network operations as another combat competency. These five core competencies together, PSYOP, CNO, EW, MILDEC and OPSEC, are critical to shaping the information environment, influencing adversaries and target audiences (TA), as well as providing freedom of action in the realm of information (Joint Publication 3-13, II-1). Together, integrated and synchronized, they are the core competencies of IO.

1. Computer Network Operations (CNO) and EW

Computer network operations is a fairly new competency that has evolved over a few decades but has had a major impact on activities in the information environment. CNO has become an indispensable element of IO. The expanded use of wireless networking, digital computing and communication, along with the integration of computers with radio frequency (RF) communications equipment contribute to its significance in IO activities. This will weaken the distinction between EW and CNO

significantly, which will necessitate a case-by-case consideration of each operation in terms of the role of each competency (Joint Publication 3-13, I-5). It is a fact that the more integrated EW and CNO are, the easier the collection, manipulation, and dissemination of information. However, that integration creates more vulnerabilities than ever before, as it becomes more difficult to protect information. Computer network attack (CNA) and computer network defense (CND) might seem to have little relationship to EW at first, but they do interact. Their interaction is becoming more apparent and important, as there is an increase in reliance on the EM spectrum in the daily use of computer networks, particularly wireless networks. Dependence on the EM spectrum as a medium to exchange information and data that are to be processed by computers is increasing. As many computers are linked electronically, it is crucial to take into account EW planning aspects during the conduct of CNA and CND. This is due to the fact that physical access to a computer is often difficult, whereas electronic intrusion might be possible. This provides a better chance for enemies to attack wireless networks and exploit them (Joint Publication 3-51, IV-7). Electronic protection is as important as CND, as friendly computer networks must now be protected from both EA and CNA.

Although EA may be used against computers, it does not necessarily mean that the activity would be classified as CNA. EW and CNA are different in that CNA is more focused on the data stream to execute the attack, while EA relies on the EM spectrum. For example, placing a virus or instructional code in a computer's central processing unit (CPU) and causing it to fail is not an act of EA, but rather CNA. On the other hand, using an electromagnetic pulse (EMP) to destroy or damage the delicate and unshielded circuitry of a CPU is an act of EA. Although they yield the same result, the way EA and CNA are applied is what separates their meaning (Joint Publication 3-51, GL-5).

Targeting computer networks or infrastructure with EA capabilities like jamming, intrusion, or physical attack will greatly disable enemy computer networks and IT-dependent systems. In the end, this slows down the decision-making process and leads adversary leaders to make incorrect or poor decisions. At the strategic and operational levels, it is important to have effective ES assets to locate, identify, and analyze such networks and technologies. EMP or virus bombs can be used to destroy or degrade the electronics of these computers and networks. Attacking computer networks is an effective

means to bringing down the economic sector and strength of a country during peacetime or conflict. CNO can be used to target not only military power, but also the other instruments of national power.

CNA can be used to support electronic jamming by generating false alarms on enemy scopes; most modern radar systems use computer and IT technology in the processing of information. Processes might include, but are not limited to, detecting, locating, and identifying the enemy electronic order of battle (EOB) and sharing that information with necessary users. False alarms interjected by CNA would make it difficult to reach appropriate decisions about the location, situation, and intent of friendly forces. If the enemy fails to realize that they are being confronted with false alarms, this can cause the enemy to make incorrect decisions while believing they are correct.

2. Military Deception (MILDEC) and EW

In his book *The Art of War*, Sun-Tzu emphasizes the importance of deception by saying, "All warfare is based on deception."(Sun Tzu 2002, 42) By definition, military deception is those "actions that are executed deliberately to mislead adversary military decision makers as to friendly military capabilities, intentions, and operations thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission" (Joint Publication 3-58, I-1). The purpose of MILDEC is to cause the adversary to take some specific actions that will contribute to the success of the friendly mission, or sometimes to cause inaction by the adversary It is clear that the purpose is not always to make the enemy act in a certain way as desired. At times, the goal is to keep the enemy inactive when they actually need to act. MILDEC and OPSEC complement each, and one is nearly always used with the other, so it is important to integrate these two core capabilities. For MILDEC to be effective it is important that the adversary decision makers perceive the information and data they obtained as correct and have full trust in their collection systems.

The relationship between MILDEC and EW becomes obvious when the mechanisms of MILDEC—which include exploiting adversary information systems, processes, and capabilities—are recognized. That relationship is growing due to the fact that militaries are using the EM spectrum for deception purposes more frequently. As the enemy employs more infrared (IR), electro-optical (EO), and radio frequency (RF)

sensors, such as radar, radar warning receivers (RWR), remote sensing, and satellite imagery, friendly forces need to use the EM spectrum to counter them. This necessitates taking appropriate electronic protection measures to reduce vulnerability.

In today's information realm, causing adversary decision makers to believe what is not true is vital for gaining and maintaining information superiority. MILDEC seeks to mislead adversary decision makers by manipulating their perception of reality and causing them to act incorrectly, make incorrect decisions, or remain inactive when necessary. At the strategic level, intelligence about the adversary and reliable and correct target analysis becomes important for a successful MILDEC, initiated during peacetime. EW is a part of this MILDEC process, and is used to detect, locate, and identify targets, and then analyze their characteristics to direct suitable MILDEC measures accordingly. ISR capabilities are especially important to intelligence and target analysis.

MILDEC can be used to influence an adversary causing them to underestimate EA, ES, and EP capabilities (Joint Publication 3-13, B-1). This can be accomplished through public affairs and civil affairs, as well as through a PSYOP campaign waged via open communication means such as the media, Internet, and television. An adversary may not take appropriate measures and precautions if they think they maintain information superiority; they will be disappointed once the conflict begins and they find they lack countermeasures because they underestimated friendly capabilities.

EA and ES can be used for, or in support of, deception measures. EA and ES degrade adversary capabilities to detect, observe, report, process, and disseminate activities within and information about the friendly information environment. That, of course, causes the enemy to misinterpret information received by electronic means (Joint Publication 3-13, B-2). Nevertheless, a strategic deception campaign might fail to succeed if it loses credibility. It is necessary to balance the relationship between EA/EP/ES measures and MILDEC.

Electronic Warfare	Supports	MILDEC	By	Misleading the enemy by manipulating their perception of EM spectrum
Electronic Warfare	Supports	MILDEC		Detecting, locating, identifying, and analyzing targets to direct appropriate MILDEC process
MILDEC	Contributes to	Electronic Warfare		Influencing the adversary to underestimate EW capabilities and thus become vulnerable
Electronic Warfare	Helps	MILDEC		Limiting the enemy to only seeing what MILDEC creates
MILDEC	Limits	Electronic Warfare		Dictating that some of the nodes and sensors will survive
Electronic Warfare	Helps	MILDEC		Shaping EOB in friendly favor

Table 8. Military Deception Relations to Electronic Warfare

MILDEC plans might limit EW, especially EA, capabilities in a way that limits the EA targeting of enemy information systems, so as to let them survive and continue their C2 functions (Joint Publication 3-13, B-5). Table 8 gives a summary of the relationship between EW and MILDEC. If everything related with information is denied to the adversary, then the adversary cannot be influenced to see, observe, report, and interpret information-related activities in the manner we desire. The electronic order of battle must be shaped to provide the enemy a false picture to act upon. EA capabilities like jamming, intrusion, and masking can not be used at all times for every target. Together with MILDEC planners, EW planners must coordinate and synchronize their efforts for the same purpose in terms of identifying which targets to apply EW to, what tools or platforms to use, when to employ EW, and how much EW to employ. Otherwise, it is highly probable that EW and MILDEC will conflict, degrading friendly capabilities and adversely impacting the mission.

3. Operations Security (OPSEC) and EW

Operations security is the process of identifying critical information and denying it to adversary decision makers to cause them to miscalculate the friendly forces, courses of action, and intentions. This leads the enemy to make incorrect decisions about the

situation (Joint Publication 3-13, II-3). Frequently, operations security complements a deception plan, and it is usually difficult to think of them separately. In the process of planning and executing MILDEC, the commander has to think about and integrate operations security. OPSEC is used to influence the adversary decision-making process through wrong, defective, or missing input.

OPSEC has three phases: identifying the friendly actions observable by the adversary, determining which friendly indicators can be obtained by adversary intelligence capabilities, and selecting and executing ways to reduce or eliminate those indicators. Each EW subdivision relates to each of the three phases to some extent, as seen in Table 9. Operations security planners should know what kind of EM spectrum activities can be seen by the enemy through EA capabilities; EP is carried out to fill the gaps in vulnerabilities so that friendly actions are not revealed or disrupted by the enemy. The development of EP capabilities also depends on intelligence collection during peacetime. For this reason, strategic intelligence collection means, such as image intelligence (IMINT), measurement and signature intelligence (MASINT), and signals intelligence (SIGINT), must be active in the peacetime environment.

	OPSEC Process	**EW Activity**
1	Identify those actions that can be Observed by adversary intelligence syste	ES measures SIGINT, MASINT
2	Determine what indicators hostile intelligence systems might obtain.	SIGINT, UAV surveillance, EW Wargaming, EW Modelling and Simulation
3	Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.	EP, EW hardening, RCS reduction (stealth technology), hard and soft EA assets (jamming, ARM)

Table 9. Relation of Electronic Warfare to Operations Security Process

Military missions that can avoid detection by enemy radar usually prove to be more effective. Radar cross section (RCS) reduction, widely known as stealth technology, first became public in the early 1970s, and RCS reduction in ships, submarines, aircrafts,

Unmanned Aerial Vehicles (UAV), missiles, and ground vehicles took priority in the design of platforms (Jenn 2005, 1). Some of the platforms include, but are not limited to, the F-117A Nighthawk, B-2 Spirit, F-22 Raptor, Sea Shadow, USS Hopper, and DD(X). See Figures 25 and 26.

Figure 25. F-117 A Nighthawk Stealth Platform (From Military Analysis Network(b) 2006)

The details of RCS reduction technology directly relate to OPSEC. By using stealth technology, many adversary ES capabilities become useless, because they are unable to detect the stealth or low-observable (LO) platforms low radiation emissions and low radar and IR signatures. At the same time, stealth platforms directly contribute to OPSEC by denying the enemy information about the platform—speed, location, direction, and other features. The US B-52 raids into Vietnam can be given as an appropriate example. In 1967, B-52 raids were being recognized by the Vietnamese early enough to endanger the raids. The problem in this case was not a classified information leakage. The enemy was cuing in on the unclassified flight plans of the B-52 crew in the international air traffic system. From that information, the North Vietnamese were able to estimate the raid entry times and the altitude. This is a great example of an OPSEC failure, emphasizing that not only classified data must be protected. Unclassified data might reveal the nature of operation as well. Related to this example, utilizing LO platforms can prevent the flight indicators from being compromised by the enemy. This is an example of the second process of OPSEC, determining what indicators hostile intelligence systems might obtain.

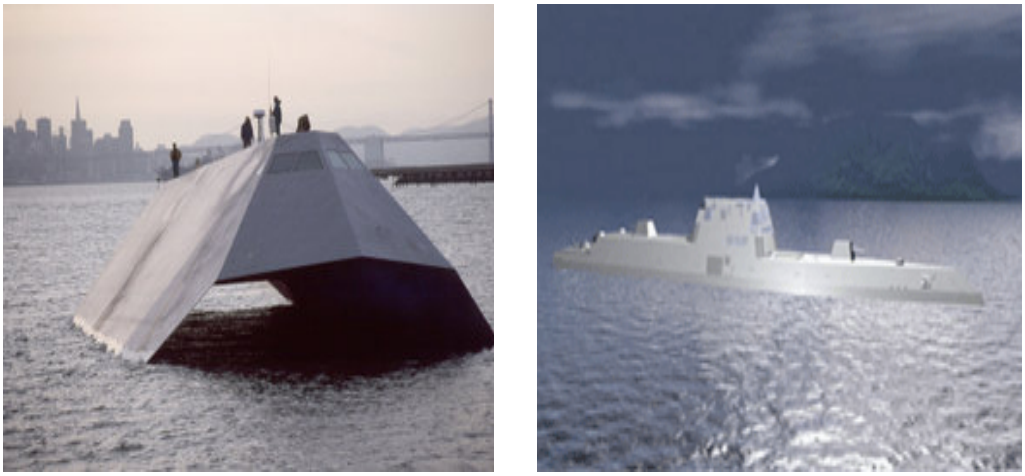


Figure 26. Sea Shadow (left) and DD (X) Stealth Platforms (From MSN Encarta Webpage 2006)

ES provides OPSEC with information about adversary capabilities and intentions to collect intelligence on essential elements of friendly information (EEFI) by means of the EM spectrum. In addition, electronic warfare support is used to augment the effectiveness of friendly emission control (EMCON) and information operations condition (INFOCON) measures and recommend modifications or improvements (Joint Publication 3-51, IV-5). The close coordination and frequent review of EEFI by the EW and OPSEC staffs is critical for adapting to a dynamic information environment.

UAVs can be used to perform electronic masking missions for tactical ground troops, which create controlled radiation of electromagnetic emissions that will protect friendly frequencies and radiation from hostile ES assets. Doing so denies the enemy the ability to collect enough data for a decision. UAVs are also used as expendable, low-cost, and commercial off-the-shelf (COTS) jamming and surveillance platforms. Dragon eye, RQ-1B Predator, and the BQM-74 Chukar are some examples of UAVs that can be used for these purposes.

Physically attacking C4ISR systems and communication nodes with either hard EA means, like precision guided munitions (PGM), JDAM, or anti-radiation missiles (ARMs), or with soft means, like jamming and probing, contributes to OPSEC by

slowing down the OODA loop of the enemy, making it difficult for the enemy to collect and disseminate enough correct information to decide and act appropriately.

Friendly systems and platforms can be evaluated with a series of operational and developmental tests to determine their vulnerabilities and assess their probability of being exploited by the enemy. To do that, available EA capabilities can play the red force and ES platforms can act as the blue force, in a kind of war game or operational exercise. EA assets attack ES platforms to find out ES vulnerabilities. At the same time employment of ES against these EA assets can also help determine the strength of ES systems and weaknesses of EA systems. EW hardening can help greatly to avoid unintended radiations and other undesirable effects of EM energy by filtering, attenuating, grounding, and shielding (Joint Publication 3-51, I-6).

The training and awareness of EW personnel with regard to OPSEC measures play a critical role. EW personnel should understand that OPSEC, having no rule of thumb, is a significant process which applies differently to each situation, and that the EW personnel and platforms must be flexible and accommodating enough to respond effectively in various conditions.

In a military deception campaign, electromagnetic deception and OPSEC must be integrated, synchronized, and coordinated in an appropriate fashion. Friendly indicators can be adjusted so that they convey incorrect data. It is important to make the adversary think the indicators are real, so that they will not continue to search for other corroborating data. OPSEC measures can conceal EW units and assets from IR and radar sensors, lasers, and EO systems of the enemy, degrading their ability to see, report, and process information. It is vital to apply EW and OPSEC in a way that they do not limit each other's capabilities and do not interfere with each other's objectives.

4. Psychological Operations (PSYOP) and EW

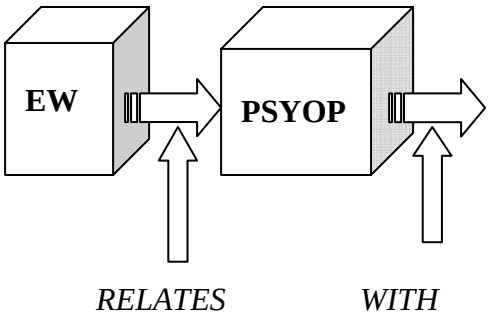
Influencing the mind of the adversary must always be the ultimate objective of information operations. This is always most important than destroying troops and equipments. As long as the troops act in a manner that friendly decision makers desire, than it is easer to win the information superiority. As discussed in the previous chapter, PSYOP disseminates true, or seemingly true, information or indicators to ultimately

influence adversary organizations, groups, and individual behaviors. To accomplish this, motives, emotions, and perceptions of the target audience should first be understood. This very broad PSYOP mission can be employed through print media and radio as well as though more sophisticated means, such as the Internet, text messaging, and other media (Joint Publication 3-13, II-1). E-mail and Web sites may also be used to conduct PSYOP.

Recent advancements in the areas of communications, electronics, digital signal processing, computer systems, and other information technologies, coupled with synergistic, net-centric application and execution, enable competencies like PSYOP and MILDEC to offer a greater number of improved capabilities (Joint Publication 3-13, I-3). This requires more involvement of EW in these areas.

EW used to be involved only in the broadcasting portion of PSYOP; however, wide use of Internet and wireless networks have necessitated more EW coordination with PSYOP efforts. This is due to the fact that PSYOP, along with the other elements of IO, is increasing its dependency on the EM spectrum as a medium to get the message to the target audience. Today, even radio broadcasting of PSYOP themes in hostile territory can be considered more difficult than before, because EA capabilities like jamming, EM deception, electronic masking, and EM intrusion are widely known and used by many countries and can disrupt the transmission. Now it is easier than it used to be to have influence on individuals and thus have strategic impacts using PSYOP. This requires an improvement of the EA-PSYOP relationship.

The actions necessary for the successful implementation of PSYOP include target analysis, reliable mediums or media for transmission, rapid exploitation of PSYOP themes, and continuous evaluation of results (Joint Publication 3-53, V). In almost every case mentioned EW plays an important role. Figure 27 presents a widened look at the EW-PSYOP relationship.



- Assessing the past PSYOP effects
- Targeting C^4ISR infrastructure
- Using enemy frequency for PSYOP activities
- Benefiting EC-130E Commando Solo platform
- Providing capable platforms and mediums for PSYOP mission
- Employing SIGINT and ES to shape PSYOP themes and the medium that will be used
- Providing reliable mediums
- Applying electronic deception to empower PSYOP messages
- Conveying show of force power by media and military exercises

Figure 27. PSYOP and EW Relationship

At the strategic or theater-operational level, the EC-130E Rivet Rider/Commando Solo PSYOP aircraft can be used to provide PSYOP capabilities in support of allied or coalition forces (Joint Publication 3-13, VII-2). Their primary mission is PSYOP and they are capable of airborne broadcast of TV and radio signals. Commando Solo is able to conduct PSYOP and civil affairs (CA) broadcast missions in the standard AM, FM, HF, TV, and military communications bands. It is used in peacekeeping, peace making, and humanitarian assistance, all of which are important missions for today's military. The EC-130E can also be used in the pre-hostile and peacetime environment where IO campaigns may be waged. The Commando Solo aircraft is shown in Figure 28.

Figure 28. EC-130E Commando Solo PSYOP aircraft (From Military Analysis Network (c) 2006)

Operational exercises in which EW capabilities are prevalent and emphasized, along with the results of successful tests of new high-tech EW assets, would certainly help to give a target audience the idea that they are outmatched in any conflict and unlikely to win. This is a potential lash up between PSYOP and EW.

Providing timely intelligence employing SIGINT (COMINT and ELINT) and ES, the military can collect new data or update existing information about the adversary. These ES reports can be used to assess the effects of past friendly PSYOP activities, although measures of effectiveness (MOE) are often difficult to establish (Joint Publication 3-13, II-5). ES indirectly helps to shape PSYOP campaigns specific to a particular area of responsibility or theater. It also helps to conduct target analysis and identifies what kind of desired messages are used by the enemy PSYOP authorities through electronic interception, assisting with counter-propaganda. Those activities might be used to construct new themes or update the existing ones.

At the operational level, enemy radar sites, radar-aided weapon systems, and C^4ISR systems can be targeted to break the bi-directional communication between commanders and troops, as well as to destroy and degrade EW capabilities. Destroyed and degraded C^4ISR systems will increase psychological operations impacts and slow down the adversary decision making process. Targeting of these systems might be done

by jamming C^4ISR systems electronically, using platforms like the EA-6B Prowler. C^4ISR systems could also be destroyed using Joint Direct Attack Munitions (JDAM) or precision guided munitions (PGM), likewise denying the enemy the opportunity to reassure troops and forward deployed commanders to counter friend PSYOP messages. Figure 29 shows a PGM hitting its target. All of these types of activities create chaos and loss of control among units, individuals, and leaders, which will eventually degrade the adversary's motives, emotions, and perceptions.

Figure 29. A PGM hitting its target (From Wikipedia Encyclopedia 2006)

EW helps PSYOP by degrading the enemy's ability to observe the activities in theater, report those activities, and make decisions accordingly. That helps to isolate the target audience from information sources (Joint Publication 3-13, B-2). Directed Energy Weapons (DEW), High Powered Microwave (HPM), and Electro Magnetic Pulse (EMP) technologies might create better results in affecting the citizens of the adversary's country psychologically while minimizing collateral damage. This decreases the adversary's motivation and will to fight for a cause and plants doubts about decision makers and leaders because of their incorrect and costly decisions.

Rivet Joint is the Air Force's primary airborne reconnaissance platform providing data to theater commanders and national command authorities. The data collected is essential for effective PSYOP operations as it helps to complete the electronic order of battle (EOB).

At the tactical level, broadcasting PSYOP products on adversary frequencies is an example of the mutual relationship between EW and PSYOP (Joint Publication 3-13, B-1). To accomplish this, ES assets first need to identify which frequencies are being used by the enemy. Then, considering friendly EA capabilities, it can be determined which of these frequencies to jam electronically. ES capabilities also help to identify how the enemy will try to degrade, disrupt, or disable our PSYOP capabilities though their own EA assets.

If frequency spectrum management is not done properly, then it is possible for PSYOP broadcasts to conflict with EA efforts (Joint Publication 3-13, B-5).The frequencies used for PSYOP must not conflict with those used for other purposes. This is ensured through the preparation of the joint restricted frequency list (JRFL), which includes taboo, guarded and protected frequencies.

The EC-130H Compass Call can be used when conducting joint PSYOP (Joint Publication 3-13, V-9). Electronic warfare—EA, suppression of enemy air defenses, and offensive counter information—is amongst the primary missions of that aircraft. Electronic deception used as an integral part of an overall deception campaign helps PSYOP messages to be more trustworthy and seemingly true. It reinforces the enemy’s misperception of the battlefield, assists in the deception campaign, and magnifies the image of friendly power in the eyes of the enemy.

B. HOW DO THE SUPPORTING COMPETENCIES SYNCHRONIZE WITH EW?

The supporting competencies of IO are physical security, physical attack, counter-intelligence (CI), information assurance (IA), and combat camera (COMCAM). These five capabilities are depicted in Figure 30. They directly or indirectly contribute to the effectiveness of IO. This section investigates their relationship with EW.

Figure 30. IO Supporting Competencies

1. Physical Security and EW

Physical security is a part of overall security precautions. It is concerned with physical measures for the purpose of safeguarding personnel and preventing unauthorized access to equipment, installations, materials, and documents. Physical security also safeguards all of these from espionage, damage, theft, etc. It also includes determining the vulnerabilities of friendly equipment, installations, and other elements to known hostile activities and systems. It differs from information assurance in that IA ensures that information and information systems are protected while physical security guards the installations and sites that possess information and information systems (Joint Publication 3-13, II-6). Protection of the information systems or any related construction is a part of physical security.

Use of a jamming device for military convoys traveling in Iraq can be considered physical security. In this example an EA capability is used to protect

friendly forces, safeguarding personnel and vehicles during troop movement. This is an example of active electronic protection using electronic attack for physical security purposes.

Even during peacetime, in almost every facility and installation, the presence of thermal imaging devices, surveillance cameras, and other security measures, in addition to security personnel, are used to ensure adequate levels of physical security. These systems and personnel must be integrated via communications into a command and control system. EP is designed into such a system to safeguard communications from enemy interference, jamming, and intrusion (Joint Publication 3-13, B-2). EP measures also degrade the effectiveness of enemy intelligence collection capabilities and deny terrorists, criminals, and unconventional forces access to sensitive communications in these facilities during conflict and peace.

Physical security sometimes requires the destruction of EW equipment, documents, assets, and platforms to avoid capture by the enemy. Such capabilities are designed into critical equipment with clearly understood instructions. For example a Special Forces team of five is ambushed by the enemy and the team possesses a combat radio that operates using national codes and a cryptographic algorithm. In this particular situation, the team has to physically destroy the radio to not reveal secret cryptology to the enemy and burn any paper or document relating to codes that are used for communication purposes.

Physical security measures are used wherever EW equipment is present. This ensures the availability, survivability, and operability of the systems or equipment (Joint Publication 3-13, B-3). Physical security is critical to the protection of radar sites, C4ISR assets, links, nodes, equipment, and the personnel that support them. Establishing personnel access rules for EW buildings, sites, equipment, and informational or instructional documents; utilizing access control devices, such as ID cards and badges; and placing entry security guards all help to safeguard sensitive materials.

Covering and camouflaging radar sites against enemy sensors, satellite imaging, and ISR is another way in which physical security contributes to EW. Other physical security measures include, but are not limited to, fencing and perimeter stand-off, lighting

and sensors, vehicle barriers, blast protection, intrusion detection systems and electronic surveillance, and access control devices and systems. Figure 31 shows some of the examples of physical security measures. Those measures should be overlapping and deployed in depth to enable multiple controls to fill security gaps (Joint Publication 3-57, VII-15). With current technology, such as retinal and iris recognition, finger print recognition, voice recognition, and face scanners, access control has improved.

Figure 31. Examples of Physical Security Measures of EW Sites and Installations

2. Physical Attack (Hard Kill) and EW

Some references use the term “physical destruction” instead of physical attack. The two are synonymous. They can also be referred to as hard-kill capabilities. Physical attack disrupts, destroys, or damages targets of any kind using kinetic destructive power; it might also be used to change the adversary’s perception of the situation in a manner favorable to friendly forces. Physical attack is not done when IO fails; nevertheless, it supports IO. Remember that IO is concerned with the ultimate objective, rather than with the manner in which forces reach that objective. Physical attack is an area that militaries are most familiar with and well-trained in. However it should not be the first thing that

comes to the mind of the commander when evaluating IO alternatives. It is true that while at first it seems easier to apply physical attack and observe concrete results, in many circumstances it can be less efficient than the application of an appropriate element of IO.

Physical attack provides an effective means of attacking adversary C2 nodes, links, communication systems, radar sites, and other portions of the EW and communications infrastructures. The destruction of those targets ultimately seeks to influence the targeted audience (Joint Publication 3-13, II-7).Physical attack can also accomplish the physical destruction of adversary EW systems and therefore support friendly EW operations superiority. As a cautionary note, in destroying enemy emitters, if not well planned, physical attack can limit friendly ES capabilities to employ intrusion or transmission analysis on the targets (Joint Publication 3-13, B-5).

Precision strike with PGMs is an important element of physical attack. Frequency deconfliction and frequency management are vital to such attacks because many weapon systems rely on the EM spectrum to accomplish their missions. ES platforms dynamically map the EM environment for targeting and target avoidance. EA carries out an important role in defeating enemy air strikes and also countering enemy PGMs. Radar and IR guided missiles; man portable air defense systems (MANPADs) (see Figure 32); Tomahawk; ARM; and HARM are some of the major systems and weapons used in destruction (Joint Publication 3-13, IV-6). HARM and ARM weapons must be deconflicted with friendly emitters to avoid fratricide.

Figure 32. Infrared Guided MANPADs Are Used for Air Defense (From Radar War Website 2006)

In addition to the systems mentioned, directed energy weapons (DEW) are gaining importance in terms of carrying out the destruction mission. Some other means to attack are airborne PGM; JDAM; cruise missiles (CM); intercontinental ballistic missile (ICBM); RF-, IR-, or EO-aided artillery; and expendable UAVs with explosive payloads.

The first two days of the First Gulf War are an example of effective suppression of enemy air defenses (SEAD) including destruction by physical attack. This was discussed in the historical perspective chapter. Iraqis were denied the use of most of their intelligence collection, communications and command and control capabilities, which enabled coalition forces to prevail in the information environment and to gain information superiority.

Figure 33. AWACS As an Example of EW In Support of Physical Attack Means (From Air Force Technology Website 2006)

ES and SIGINT help to locate, classify, and prioritize targets for physical attack. This shortens the targeting cycle. Emission control (EMCON) and ES are important in protecting friendly assets from enemy PGMs. ES provides enough time to react against such attacks and disable the electronics of the missiles. ES also provides feedback on the results of physical attack by analyzing the communications and emissions traffic and density. In other words, ES makes an electronic battle damage assessment (BDA) through the use of SIGINT and ES capabilities (Joint Publication 3-51, IV-7).AWACS, (see Figure 33 above) JSTARS; and U-2 are some examples of ES capabilities appropriate for such SIGINT missions.

GPS uses satellite signals to determine position, velocity, and direction. GPS and precision navigation and positioning (PNP) give modern weapon systems the ability to precisely attack selected targets, which minimizes collateral damage. GPS and PNP contribute to the effectiveness of targeting and munitions control, as well as reduce the number of sorties required to destroy or degrade a target (Air Force Doctrine Document 2-5, 34). It is important to emphasize that collateral damage can be used as a propaganda asset by the adversary to increase the will of the populace to fight and to reduce friendly PSYOP influence over them. Such propaganda might have lasting effects beyond the current conflict.

3. Counter Intelligence (CI) and EW

CI is comprised of collected information and activities performed to counter adversary intelligence, espionage, sabotage, assassinations, etc. Only careful coordination of CI with OPSEC, physical security, and IA ensures the protection of information and information systems (Joint Publication 3-13, II-7).

CI supports EP and ES by providing electronic countermeasures (Joint Publication 3-13, B-3). EP and ES assets must be allocated appropriately to ensure accomplishment of both EW and CI activities. EW means can be used to destroy or degrade enemy intelligence capabilities. Electronic masking of activities in the EM spectrum, electronic deception of enemy intelligence sensors, electromagnetic hardening, and EMCON and electronics security are all potential counter-intelligence activities. ES measures can help to search for, intercept, classify, and localize potential hostile emitters (Joint Publication 3-51, I-8). Some EW and communications platforms may be used to rapidly disseminate collected enemy data and intelligence to assist in timely and accurate CI activities. To be able to accomplish this, friendly EP must be capable of operating in the adversary electronic attack and electronic warfare support environment.

Electronic intelligence collected through SIGINT and ES capabilities is used to evaluate, analyze, and update enemy intelligence capabilities. This helps to reorganize and update friendly CI activities and direct them to the appropriate enemy capability.

4. Combat Camera (COMCAM) and EW

The mission of COMCAM is to provide leaders, commanders, and decision makers at all levels with imagery to support operational and planning requirements (Joint Publication 3-13, II-7). The acquisition and utilization of imagery can be still or motion, and can be used in support of combat, information, humanitarian assistance, special force, ISR, engineering, legal, public affairs, and other operations involving the Military Services (Joint Publication 1-02, 97).

ES capabilities that support intelligence also contribute to the COMCAM mission across the spectrum of conflict. Motion and still imagery can be used to locate, identify, and analyze radar installations, surface-to-air-missiles, and other potential EW targets.

COMCAM can be used to assess the effectiveness of EW hard or soft targeting by providing imagery of targets as a form of battle damage assessment (BDA). EP contributes to the COMCAM mission by enabling safe transmission of COMCAM imagery.

5. Information Assurance (IA) and EW

IA is composed of measures that protect and defend information and information systems. These measures provide and ensure the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems. IA is an indispensable element to gaining information superiority. IA relates to EW in that EW provides operational protection against adversary and intelligence efforts that target friendly electronic information and information systems (Joint Publication 3-13, II-6). IA is concerned with information itself—whether it resides in a computer, network, cable, or is radiated via the electromagnetic environment. Reliance on computers and IT to conduct EW increases the challenge to pursue effective IA. IA is one of the competencies insuring EW assets are readily available and accessible (Joint Publication 3-13, B-2). Incorporating the compatibility, interoperability, survivability, and supportability of EW assets and platform designs ensures an effective and affordable level of information assurance activities

On the other hand, EW supports IA through EP by protecting the information, information systems, and assets (Joint Publication 3-13, B-3). Controls and measures, such as communications security (COMSEC) and emission control (EMCON), can be used to deny the unauthorized user access to EW or information systems. This provides telecommunications authenticity and prevents the unauthorized user from deriving intelligence using telecommunications means. Activities such as cryptology, transmission security, emission security, and physical security of communications and EW assets and information can be considered IA. Password authentication and encryption methods are possible ways to deny unauthorized user access. EW personnel should be well-educated about the importance of IA in protecting assets from hostile activities.

C. THE PA, CMO, AND DSPD RELATIONSHIP TO EW

The IO related competencies are public affairs (PA), civil military operations (CMO), and defense support to public diplomacy (DSPD), as shown in Figure 34. These

capabilities, while related to and requiring coordination with IO, are distinct and must not be compromised by IO activities (Joint Publication 3-13, II-8). The relationships between EW and these supporting competencies are ambiguous and indirect for the most part.

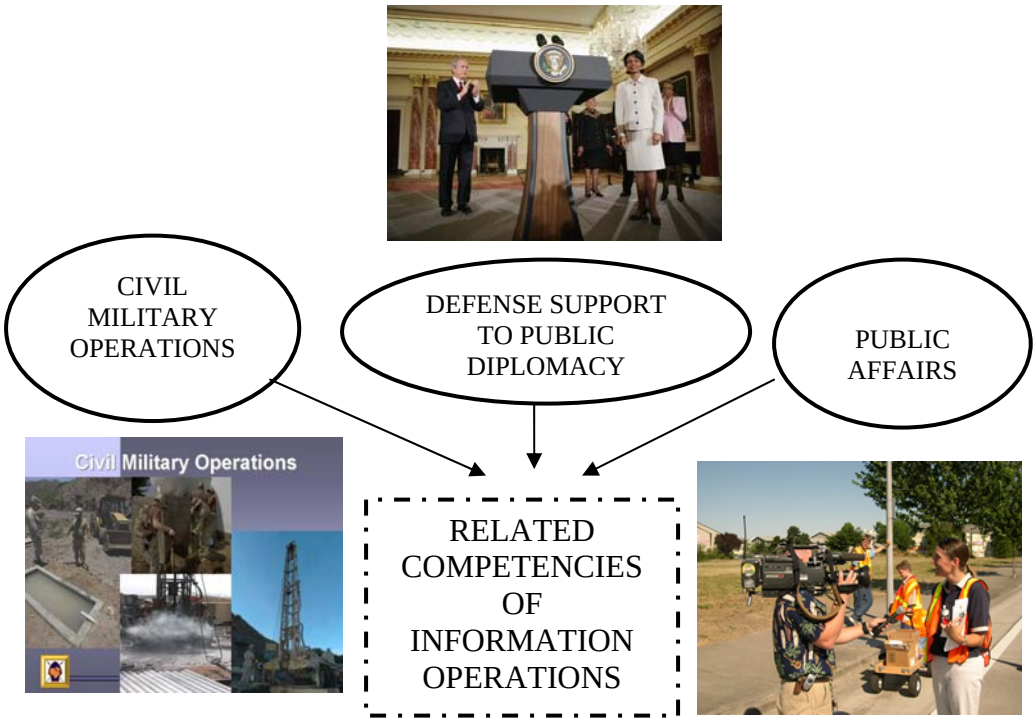


Figure 34. Information Operations Related Competencies

Public Affairs (PA) is defined as "public information, command information, and community relations activities applied to internal or external audiences" (Joint Publication 3-13, II-8). ES and EP capabilities that enable communications between PA authorities and their audiences support PA. ES, EP, and necessary physical security measures help ensure continuous media coverage and prevent physically and electronically unauthorized access to the equipment and sites used for PA purposes. Around-the-clock availability of live and broadband broadcasting ensures that PA activities can be performed at any time they are needed.

News media can be used to support EW activities in the accomplishment of military objectives. For instance, through news media, integrated EW exploitation during joint exercises can be emphasized, successful missile interception tests and exercises can be covered, and friendly EA capabilities like jamming and spoofing may be used in

headlines that ultimately influence decision makers and convey an image of the friendly forces' strength. In addition, using the PA medium, DEW, and high-power microwaves (HPM) can be advertised, and it can be explained that collateral damage is minimized and civilian casualties are reduced by pinpointing only military targets.

It is important to deconflict PA and EW so that they do not interfere with each other and they do not limit the accomplishment of their separate objectives. In this sense, electronic warfare support can help locate, identify, and then analyze the adversary communications mediums appropriately and then set the suitable PA channels. For example, it is no use to use television as a public affairs medium if the targeted audience does not have a television to watch.

Defense support to public diplomacy (DSPD) includes measures and activities taken by DOD components to support and facilitate public diplomacy efforts. DSPD seeks to inform, influence, and broaden the dialogue between U.S. and foreign countries (Joint Publication 3-13, II-10). COMCAM activities that involve EW activities can also be used in DSPD to provide responsive imagery coverage (Joint Publication 3-13, B-9).

Like public affairs (PA), DSPD can be used to show friendly EW capabilities—electronic support (ES), electronic protection (EP), and electronic attack (EA)—and can cause the adversary to lose the will to fight. EP and ES protect the medium by which the DSPD message is conveyed from adversary EA capabilities. Aircraft such as Commando Solo can also be used for DSPD purposes. EP and EA can be used to protect diplomats and political figures when they are in a war zone or in hostile territory from physical attack or communications intelligence by the adversary.

Civil military operations (CMO) are the activities of the commander that establish, develop, and sustain positive relations between governmental institutions, non-governmental organizations (NGO), civilian authorities, civilian populace, and military forces (Joint Publication 3-13, II-8-9).

The establishment of a training and exchange program for EW equipment and systems improves the relationship between friendly forces and their allies during post-conflict reconstruction. Operators, EW staff, and engineers of allied nations can all receive valuable training with each other's help. To sustain positive relations, allies can

equip each other with personnel and systems when confronting a shared enemy. For example, friendly forces can donate early warning radars or air-defense artillery weapons to each other and train operators for each other's systems.

EP helps to protect the frequencies used for CMO purposes. This frequency spectrum management ensures the availability of communication mediums for CMO purposes. In crises or post-war environments, allies can help to reestablish local and governmental agencies and restore command and control functions. By focusing on restoring ISR capabilities and communication links, the EM environment can be rebuilt.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND IO-EW CONSIDERATIONS FOR TURKEY

This chapter discusses IO and EW considerations for the nation of Turkey. The ideas in this chapter represent the author's personal opinions and are derived as a result of his pursuit of a Master's Degree at the Naval Postgraduate School (NPS) in Monterey, California, and his comprehensive research on behalf of this thesis. None of these conclusions are to be construed as scientifically proven analyses. They reflect the author's application of his knowledge and thoughts about the areas of IO and EW gained during his studies at NPS, applied to the specific environment of Turkey. The considerations presented in this chapter are grouped into areas of personnel, training and execution, and technology.

A. IO CONSIDERATIONS FOR TURKEY

It is largely acknowledged that the world is living in an "information age" in which achieving information dominance and decision superiority has become increasingly important. Information Operations (IO) is proving to be a useful tool for nations to employ. This applies to Turkey in much the same way as it does the United States.

After the Cold War, Turkey emerged as one of the most powerful and influential nations in its region. As a long-standing NATO member and strategic partner of the United States, Turkey has been involved in numerous regional and strategic crises and conflicts, including but not limited to Bosnia, Albania, Kosovo, and lately a commanding role in Afghanistan.

Today, small unit and special force operations have gained great importance. Operations in the modern day have transformed from being human-centric to technology-centric, which enables nations to reach their objectives using small but technologically advanced units rather than brute force or overwhelming power. These modern realities emphasize the importance of IO for Turkey; therefore, Turkey has adapted IO concepts to its own particular situation and has begun evaluating the application of IO for both civilian and military purposes.

Personnel

Implementing IO requires that different personnel and organizations play their roles in an orchestrated manner. The actors are not only the military, but also political leaders, government agencies, and civilian organizations—any individual, organization, or agency that might influence the decision-making process. Therefore, maintaining enough expert personnel with the proper qualifications is important to implementing and sustaining the power of IO.

From time to time, IO might impose organizational changes to government agencies and the Armed Forces in order to promote and facilitate coordination and integration. Therefore, Turkey might always be in need of some organizational changes. In a constantly changing, information-dominated world, the status quo is likely to lead to stagnation. Such changes and their impact on the overall effectiveness of national power must be carefully evaluated before they are applied. Turkey will benefit by continuing careful analysis of the integration of IO into the organizational structures of other nations. It is important that Turkey investigates the difficulties other nations encounter and applies IO in a manner that appreciates the unique nature of its own structures.

IO contains broad areas of application that include soft-kill and hard-kill aspects. Older conventional warfare capabilities that are a part of IO, such as MILDEC and PSYOP, and the newer sophisticated technologies, such as EW and CNO, must go hand-in-hand within IO. To best and most efficiently conduct synchronized IO, there must be a requisite number of experts in each of these areas or "capabilities" of IO. Only after this requisite number of experts is gathered can IO be applied appropriately. Therefore, personnel recruiting, education, and allocation become crucial and must be continually monitored.

All civilian and military personnel involved in decision-making processes must have sufficient knowledge of IA, OPSEC, physical security, and CI competencies, regardless of their primary area of expertise and job title.

Training and Execution

To be better prepared for the conflicts of the future and the uneasy peace between them, Turkey would benefit from closely monitoring IO research and related developments around the globe. Turkey must especially consider continuing to participate with its friends and allies in these areas and continue to make efforts in training its government and military personnel in the areas of IO.

The current emphasis on training individuals in IO should continue. Training becomes more efficient if it is given to individuals and groups at every level of hierarchy and occupation in a balanced manner. This balanced approach can increase IO effectiveness because strategic and operational IO planners and decision makers can better evaluate situations, and in turn guide tactical planners and commanders more effectively. Likewise, tactical IO decision makers can better understand what is demanded by their superiors and implement results with more accuracy. Such training can be conducted via seminars, briefings, military exercises, and lectures, adjusted to the specific needs of each group.

One of the strengths of IO is that it can be implemented by a country that does not have the ability to adopt exotic and sophisticated IO technologies, such as those common in the capabilities of EW, CNO, and advanced physical attack. IO can transform the combat and diplomatic power of a nation by weighing each competency according to the specific capability of that nation against those competencies of an adversary. This transformation extends its applicability and power across the full spectrum of peacetime, crisis, war, and post-war periods. Turkey can benefit from the power of IO by using it flexibly to conduct humanitarian assistance missions, United Nations missions, NATO duties, civil military activities, refugee relocation assistance missions, and diplomatic processes.

Information Operations blurs the lines separating strategic, operational, and tactical levels of warfare. In a world of rapid communications that is inundated with information, tactical mistakes may result in operational or strategic failures. Also, problems and difficulties encountered during IO planning phases may impact execution at all three levels of warfare. IO blends these three levels of warfare and the decision-

making processes that support them and tie them together. Coordination between these levels of command and control is critical. It is important to increase the frequency of the meetings (electronic or physical) where strategic decision makers meet with operational and tactical commanders and their staffs. These meetings are necessary because IO issues can be addressed and coordinated, and potential solutions to the various issues that cross the levels of command can be derived.

By itself, there is no IO. IO is not a separate force or activity. As long as people live in a world hungry for information, it is unlikely that the importance of IO will lessen. Therefore, it is important for Turkey to continue to maintain its IO perspective, recognizing it is inherent to all military and civilian activities, but not as a separate force.

Turkish Republic has always followed the guidance of its founder, Mustafa Kemal ATATURK, who said, “Peace at home, peace in the world.” Despite its strategic geographic location, Turkey has not been directly involved in any conflict over the last three decades, excluding the struggle against terrorism. Major conflicts in the second half of the 20th century through the present have occurred in close proximity to Turkey. Some of them are the Second World War, the Afghanistan-Russia War, Arab-Israeli Wars, and the First and Second Gulf Wars. Due to its close proximity, Turkey has been indirectly involved and impacted by these conflicts to some extent. At times, Turkey has granted basing privileges for combat aircraft operating out of its territory. During and after conflicts, refugees flooding across Turkey’s borders from neighboring countries have been accommodated. Some consequences cannot be dealt with easily or solely through conventional warfare strategies. IO is a good tool to be utilized in these instances. Turkey can utilize the competencies of PSYOP, defense support to public diplomacy (DSPD), CMO, PA, and combat camera (COMCAM). These competencies can be used to exploit the situation in Turkey’s interest and to deter potential negative consequences. IO can help to establish and maintain good relationships with neighboring countries and remote friends and allies.

Turkey incorporated IO into its doctrine and training quickly and has lately published the MT 411-1 and MT 145-1 Field Manuals. These have contributed to the understanding of IO concepts. It might be helpful for Turkey to investigate the new

insights on IO that are included in the recently released document Joint Publication 3-13 "Information Operations (13 February 2006)" and "Information Operations Roadmap", which are currently the leading IO joint publications for the United States military. There are changes in the categorization of IO competencies incorporated in the IO spectrum. It can be analyzed carefully for the particular needs of Turkey and then adapted as necessary.

Turkey has successfully established close relationships between universities, civilian organization, military agencies, and governmental agencies. The interest in improving these relationships in positive and scientific ways is crucial for success, as the number of actors involved in the decision-making process has increased along with the complexity of this process. The methods for handling this complexity and for achieving information dominance involve a thorough understanding of IO and careful implementation of it through coordination, synchronization, and integration of all of the different competencies, focused on the common national objectives.

IO requires different types of training, each of which is equally important. Some training is specific and extensive, such as the education of personnel in areas of CNO and EW. This is due to the high level of technological expertise that is required. Such training is often of a classified nature. Other types of training are not highly technical and have a broad application to all personnel. These areas include OPSEC, IA, and physical security. It is vital for success in IO that all personnel involved in decision-making processes receive this broader training.

Turkey has been combating terrorists for more than quarter of a century and still faces a significant terrorist threat. Turkey has made great advances in countering terrorist activities, yet there is still much to be done. IO can assist in increasing the efficiency of the country's capability to protect its citizens and resources from destructive and separatist terrorist activities. IO manages resources in a productive way through coordination and integration. The capabilities of civil military operations (CMO), psychological operations (PSYOP), and EW are synchronized under IO, increasing the efficiency of governmental intelligence collection and police activities.

The increasing impact of public affairs (PA), the power of the media, and the Internet should all be given special interest. Public affairs and the media have become more important than ever because it is increasingly easier and cheaper to gain access to them. They are used or manipulated by countries, civilian organizations, and terrorists to constantly shape the information environment in their favor. These tools are powerful because the probability of conveying messages to the targeted audience is high, access to them is easily obtained, and they do not require a high level of expertise to use. Turkey should continue implementing these tools in the best manner to eliminate or counter adversary messages conveyed through PA, media, and the Internet. These tools can be used to convey official Turkish messages to the targeted audience. It must be remembered that PA and power of media can be enough to show a success as a failure and a failure as a success.

Technology

Technology that is used in the IO competencies, particularly in CNO, EW, and physical attack, is changing rapidly. Old technology is quickly becoming obsolete. Technology that is obsolete and inferior to the technology of the adversary may not be able to accomplish the mission. This is very important in terms of acquisition programs of both military and governmental agencies.

Special interest should be given to the computer network operations (CNO) competency of IO. This competency is comprised of rapidly changing information technologies (IT), creating exploitable opportunities and critical vulnerabilities at the same time. IT is becoming inherent in every technological area; it resides in each and every competency, which makes them vulnerable to computer-related hostile activities. Although it imposes vulnerabilities upon the other IO competencies, it is a fact that, if used appropriately, CNO greatly contributes to the effectiveness of that particular competency. This is also true for Turkey.

B. EW CONSIDERATIONS FOR TURKEY

Turkey has long realized the importance and effectiveness of EW and utilized it to counter terrorist activities within its borders. There is a direct correlation between EW

and success in counter-terrorism. EW is also important for Turkey as a force multiplier. Any future crisis that Turkey might get involved in is likely to have an intensified EW dimension.

EW requires the most recent technology, and this technological edge must be held over potential adversaries. The importance of EW must continue to be emphasized and close cooperation between national industry and military and governmental research organizations should continue.

Personnel

A balanced approach to personnel recruiting and training in all three subdivisions of EA, EP, and ES is always necessary. These three subdivisions are similar to the three legs of stool—if they are not balanced, then they will not provide the necessary support.

The increased use of computers in EW systems and platforms and the minimization of human interface in most of these systems provide an emphasis on software creation and reprogramming. These two areas have very unique roles in modern EW, and it is essential that Turkey maintain emphasizing them. Having requisite software personnel working in EW assets and systems development is critical.

EW has already necessitated some organizational changes in Turkey concerning the use of EW units and resources and their partitioning between the services. It is likely that the continuously changing technology of EW will require additional organizational changes in the future. If executed carefully, those changes can increase the effectiveness and efficiency of EW activities and its overall contribution to the other IO competencies.

It is critical that Turkey always stays abreast of the latest changes in the technologies within electronic warfare subdivisions and develop the necessary technical infrastructure to adapt to these changes. Engineer or expert exchange programs and participation of EW-related personnel in bi-lateral or multi-national military exercises are possible ways to continue modernizing and evolving Turkey’s EW force structure.

Training and Execution

As EW is becoming more intrinsic within military and civilian activities, the training and education of EW must continue to emphasize future needs for using the electromagnetic environment.

Every country classifies EW-related doctrine, documents, technologies, and tactics. Hence it is often difficult to obtain this kind of information directly from the source. This aspect adds an even more complicated dimension to the difficulty in obtaining access to technological development and changes. That is why having the capability to develop EW technology and assets become more crucial for success. While taking appropriate precautions, such as complying with information assurance and physical security measures, Turkey has to continue development in EW.

The employment and capabilities of the same EW assets differs from environment to environment. For example, maritime environment search and detection radar does not have the same specifications as air defense search and detection radar. Similarly, the mountainous regions of Turkey are a limiting factor to the employment of EW. In these regions, line of sight (LOS) is limited, the transportation and movement of the systems are difficult, and seasonal conditions are extreme; very hot in the summer and very cold in the winter. In every system developed domestically or acquired from foreign countries, it is vital that Turkey continue giving special consideration to their utilization throughout these geographic regions.

Having confronted terrorist activities for more than a quarter of a century within its own borders, Turkey has gained experience on how to counter terrorism. EW has proven its potential in combating terrorist activities. This has encouraged deeper research and development in this area. EW-related terrorist threats are increasingly common. Terrorists can obtain commercial-off-the-shelf (COTS) technologies cheaply and easily, using them to improvise weapons. One example is the increased use of improvised explosive devices (IED) and remotely detonated road mines and bombs. In 2006 Turkey has experienced an increase in the use of IEDs and remotely detonated road mines (cell-phones are usually used for detonation). This shows that terrorists are also increasing their technological expertise. EW can be used to counter these types of weapons; one

example can be use of jammers with convoys to disable remote electronic controllers. Therefore it is inevitable that Turkey will continue researching the best employment of these technologies against terrorism.

The training of civilians in EW is also important. Protection of civilian aircraft and other modes of transportation against terrorist activities, electronic hardening of civilian governmental agencies, and protection of electronics against high-powered microwave weapons are some examples of how EW is applicable to the civilian sector. Training of civilians can help determine the vulnerabilities of civilian organizations and assets and can help to develop necessary protection measures.

All EW-related personnel should be trained continually about IA and need-to-know principles. Such training becomes more important when operating in an international environment, such as in bi-lateral or multi-national exercises and operations. It is crucial to protect national technology, tactics, and doctrine related to EW.

The effectiveness of EW personnel is improved when they have knowledge of the three subdivisions; it is difficult to be a good ES or EP expert with no knowledge of EA applications and theories. The interrelationship between the three EW disciplines requires knowledge in all three areas to effectively perform within one.

Being a core competency, the synchronization of EW is very important to IO efforts, as was investigated in this study. The technical side of this relationship, the most efficient employment of EW within IO activities and their limiting effects to each other, can be investigated and discussed in seminars, briefings, and lectures in Turkey.

Technology

Looking backward with a historical perspective, the conduct of EW during Operation DESERT STORM was far greater than what could have been predicted purely from the U.S. experience during the Vietnam War and prior conflicts. EW is increasingly integrated within military operations. It is certain that for the next conflict that Turkey might be involved in, there is going to be a very intense EW dimension. It is imperative that Turkey continue to emphasize EW research and development. Computer network

operations (CNO) and information assurance (IA) are unique and crucial areas that must be emphasized, as they relate to EW significantly.

When purchasing an EW system from abroad, operational test and evaluation (OT&E) of the particular system is critical. The following requirements must be examined to determine the capability of the system with regard to Turkey's needs:

- Do performance specifications match national needs? Possibly being built for the producer's operational environment, can the system accomplish the mission as desired in the operational environment of Turkey?
- Is the system interoperable and compatible with the existing systems and platforms in Turkey? What are the challenges to system integration?
- As EW technology is constantly changing. Therefore are the hardware and software of the system upgradeable, and is its documentation clear?
- Does the system have an open architecture that can be modified according to future mission needs?
- Does the system need a specific logistics support structure? Is the current structure suitable for maintaining logistics support?

Intelligence on the latest technological developments in EW is important for Turkey. Being a regional power, it is crucial that Turkey continually update its information on the latest research. When necessary, technology transfer from leading countries in EW can be utilized to acquire the latest improvements, but this is not always the most efficient mechanism. Turkey must also continue to collect intelligence about the EW potential of neighboring countries, which can be a key factor in any possible future crisis.

Turkey's development of national EW software, cryptology, and platforms has been improving in the last decade. Lately, these improvements have even begun challenging the world market. This has come about through the government's and the military's realization of the importance of this area, resulting in increased budgets for research and development at organizations like HAVELSAN (the Turkish acronym for Aviation Electronics Industry), ASELSAN (the Turkish acronym for Military Electronics

Industry), and TUBITAK (the Turkish acronym for Turkey Science and Technology Research Organization). Turkey has continued to emphasize EW software, cryptology, and platforms, and is establishing new organizations concerned with the different disciplines of EW to achieve domestic market competence and to lead more development.

Encompassing rapidly changing technologies, EW is similar to a very competitive cat and mouse game. It exhibits the characteristics of a constant race between EW disciplines. Each capability constantly tries to gain an advantage over the others. Therefore, the specifications of a platform or systems within a five-year acquisition program, for instance, may be obsolete by the time of delivery. This requires constant feedback from within EW technologies, a focus on future EW requirements prediction and careful monitoring of EW systems and platforms acquisition programs.

EW is a crucial part of military exercises. EW integration to wargaming, military exercises, and combat scenarios must continue. The scenarios can be constructed in two ways. First, EW can be utilized as the primary tool for the scenario and evaluation of EW capabilities and assets can be performed; this can be done using modeling and simulation (M&S). Second, within military operations, EW can be utilized only as a small part of the overall exercise, which helps evaluate mutual impacts, both positive and negative, of EW during military operations.

C. CONCLUDING REMARKS

The art of warfare has changed greatly; on today's battlefield there are many more dependent, independent, and inter-dependent variables. Obtaining information dominance and decision superiority is at the heart of all warfare activities, no matter what kind of technology is used. Warfare is becoming more complicated due to its constantly changing face; modern warfare requires combined arms interoperability, coordination of branches in a particular service, integration between services, and even cooperation of other military and perhaps civilian agencies. Understanding the unique interactions between the capabilities and vulnerabilities of the IO competencies is critical to success and the attainment of the ultimate objective. This thesis makes conclusions in two areas: the advantages and disadvantages of IO and the relationship of electronic warfare to IO.

The military or government objective of any conflict is to ultimately achieve the national political objectives. IO is a critical tool in this regard for the following reasons:

- Decision-making processes are the source of each and every action in human life, whether it is economic, military, or political. These processes are necessary during times of war and peace. As the ultimate objective of IO is to influence the adversary's decision-making processes and protect the friendly decision-making process, this flexibility gives IO a very broad area of action.
- IO has the capability to integrate the elements of national power—political, economical, military, and informational—to achieve national objectives.
- Conventional warfare is often applicable during conflict; however, IO possesses the potential to be applied throughout a broad spectrum, from peace to pre-hostility, crisis, war, post-war, and back to peace. Properly applied, IO considers the consequences of the battle beforehand and acts accordingly. This helps to avoid adverse consequences of warfare, such as collateral damage, excessive civilian casualties, and continuing national hatreds.
- IO brings together not only the hard-kill capabilities of military operations, such as precision-guided bombs and ARMs, but also soft-kill capabilities, such as jamming, spoofing, and creating false targets. These capabilities, if coordinated, integrated, and synchronized carefully, are able to accomplish more than any one by itself.
- Defense support to public diplomacy (DSPD) and public affairs (PA) are among the related competencies of IO. These two competencies can be used to prevent a conflict by employing political and diplomatic processes.
- IO is not a rule of thumb. In other words, it is not a concrete doctrine that applies equally to every situation. IO is an evolutionary process that emphasizes the vitality of information in the information age. That idea

enables IO to evolve its concepts, change its doctrine, and stay up-to-date as technology and tactics change.

- Influencing the adversary's decision-making cycle and protecting the friendly decision-making cycle receive equal emphasis under IO. It is a benefit of IO that it focuses on the protection of the decision-making cycle as much as influencing the adversary's cycle by employing physical security, information assurance (IA), computer network defense (CND), electronic protection (EP), electronic warfare support (ES), operations security (OPSEC), and military deception (MILDEC).

At this point a question might come to mind. Does IO have any disadvantages? Yes, some disadvantages or difficulties reside in the application of IO. Some of these are:

- IO education is difficult as it encompasses not only the military, but also civilians, political decision makers, and many other levels and structures of government and society. The interpretation and application of IO theory will vary according to the level, background, interests, and position of the individual.
- As IO is a fairly new concept, the militaries in different countries understand and apply IO differently—if they have any IO considerations at all. Therefore, it is difficult to employ IO within a coalition force structure.
- By itself there is no IO. IO is the synchronization, coordination, and integration of every information action that is done to achieve objectives. There is not one set of IO procedures that applies to every situation.
- There is risk involved in coordination and integration of the actions of each competency if it takes too much time to reach a decision or to apply the decision in the real world. It can cause the loss of information superiority over the enemy and a slow down in the decision-making cycle.

- As information systems and technology become more integrated into both military and civilian environments there are more opportunities to exploit them. These opportunities contain inherent vulnerabilities that are subject to hostile activities.

EW is a significant tool of IO and is also considered a core element. As explained in the historical perspectives of EW in this study, the first application of EW occured almost a century before the origin of IO theory and doctrine. As shown in the historical perspective, EW is becoming an indispensable element to be integrated with every other discipline of warfare, as they increasingly rely on the use and exploitation of the electromagnetic environment.

As this study reveals, the relationship between EW and each IO competencies is not consistent across the core, supporting, and related competencies. The EW relationship to IO is strongest with the core competencies.

EW is a force multiplier and requires considerable expertise. EW experts should be capable of integrating different elements of systems, have either engineering or operational experience, and be knowledgeable about the other elements of IO to be able to do their mission more efficiently.

In any applications of IO, personnel working in different IO competencies should consider EW aspects in their disciplines. To accomplish this, the mutual relationship of EW and each competency should be thoroughly investigated as new technologies are included within IO processes.

As seen in the investigation of the EW relationship to IO, use of some IO competencies might limit the usefulness or effectiveness of EW and vice versa. When conflict occurs, it is most likely that the interference can degrade the overall effectiveness of IO as well as the goal of the specific competency. This is an important point to consider in coordination efforts during IO planning and execution phases.

During EW education and training, the overall place and role of EW within IO should be taught. This kind of training helps personnel to understand the roles and

missions of EW in the IO framework and also shortens the coordination and integration time with other competencies.

Rapidly changing technology must be incorporated into IO efforts. This can be a cumbersome process if IO is not fully ready to accept and integrate those changes. The faster this is done the more efficient IO efforts are going to be.

D. FURTHER STUDY RECOMMENDATIONS

This thesis identifies many issues for further research. The following is a list of a few of these issues. A continuing investigation into these areas can increase the understanding of the evolution of electronic warfare and information operations doctrine, capabilities, and practice.

- How do technological developments affect IO and how can they be integrated into IO?
- What can be done to standardize IO across the branches, services, and perhaps nations?
- How can the problem areas of coalition forces conducting joint IO around the globe be solved?
- What is the best way to educate and train IO personnel?
- Is there a need for IO organization or a structure to employ IO?
- How do other IO competencies limit or influence EW activities?
- What is the difference between IO applications during peace, war, and post-war periods?
- Is there a need for “IO troops” and specific IO organizations? Or is treating it as being inherent to all activities the most efficient method?
- Does IO use the available EW tools or can it actually dictate or derive the technological developments related to EW?
- Is there an optimum balance between the exploitation of opportunities and protection of vulnerabilities? How can that balance be achieved?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

This appendix is the interview by 1LT Ali Can Kucukozyigit (Turkish Army) with Dr. Daniel C. Boger, Chairman of the Information Sciences Department at the Naval Postgraduate School (NPS) in Monterey, California. The interview focuses on Information Operations (IO) concepts.

1. What was your involvement with Information Operations during your military and civilian career?

I did have a relatively short military career during which I was interested and involved in Command and Control (C^2) issues, to include C2W that is now known as Information Operations (IO). I have also been interested in Electronic Warfare (EW) and IO issues ever since I have started working here at the Naval Postgraduate School (NPS). My thrust has been how we can put together and integrate a plan to support the commander. That has been my primary area of interest.

One of the things that I have watched over the years is what components of the definition of IO for the U.S. DOD have been included and which ones have not. We went through a phase a few years ago where physical destruction was defined as part of IO/IW, but of course it now has been taken out. It is a related/supporting competency at this point. It has been really interesting to watch the definitions change and the reasons for the definitions to change over the last few years.

2. What are the things done at NPS in terms of educating IO warrior of today and the future? What are some practical applications experimented in IW department in terms of IO?

The most important thing is try to get across to the students; yes there are important technical aspects that support IO and IW. But what we really want to focus on is what is happening in the mind of your adversary commander. That is what you want to change. We need to have effects and change his mind whether that is a military commander or a political leader. So consequently things like modeling particular

situations are important, not only the technical aspects of what is occurring in EW, CNO, etc., but also how the people really make decisions; how we can really affect those decisions is also important .

One of things that we got started couple of years ago and got going recently again is situational modeling, which is really an attempt to set up a network of effects and investigate how those effects are interrelated to bring about a change in the perception of the commander. We do have a number of models available in that area that are focused on human decision makers. An important way that the educational program here at NPS is structured is trying to get students to understand that the technical and the soft side have to blend together in order to create the effects that you want.

3. What would you think is the ultimate objective of IO operations? Is machinery like computers or humans?

Clearly what you want to do through IO is to change the perception of the adversary commander. It is really oriented towards humans and that is what makes it so hard to implement.

4. What would you say as a reason recently that made IO get more popular and more important?

It is because, I think, people have recognized that it is really the effect that you want to create on your adversary and not how you do it. The other reason is the recognition of everyone that we live in a net centric world where we are all connected not only physically but also electronically, socially, etc.

5. Do you have any idea of the first examples of IO conducted in history?

I like to go back to Sun-Tzu and read his comments. The Art of War is an interesting book. Everybody who has anything to do with IO should take a look at it. What he was concerned with is effects and what is going on in the mind of your adversary. There is an interesting example of the Trojan horse in history, also.

6. How did IO evolve from C2W and IW, what are the similarities and the differences between the three?

C2W essentially was a fairly technical approach to the problems; it was merely viewed as Electronic Warfare Support (ES), Electronic Attack (EA), and Electronic Protection (EP) type of activities or other activities in the light of those. Using those, you can develop a technical system that will counter any effects that the enemy wants to have on you. This would allow you to counter any C^2 systems that existed.

C2W evolved over the years to include the fact that it really is the commander that we want to affect along with his staff and major leaders. It was the recognition of people who worked C2W that there is a lot more to the problem than just being able to build that counter to the electronic portion of IO.

The Navy still uses Information Warfare (IW) terminology. What they mean by IW tends to focus on CNO and EW as the most important elements of IO. They are coming around slowly to the recognition that OPSEC, MILDEC, PSYOP, etc. are also important; that recognition is due to the push from higher levels.

There is one important point that we need to recognize. That is we are always doing IO. But we are not necessarily always doing IW. We probably do real IW only during wartime. That is an important dimension.

7. In what ways is EW used in IO and what is the mutual relationship between the two?

If you look at the three elements—EP, ES, and EA—it should be obvious to anyone that those are necessary in any sort of IO campaign. The electromagnetic spectrum is so important these days in modern militaries that you have to have EW components in your campaigns. If you don’t, you are doomed to fail.

8. Would you please comment on the differences between IO and kinetic/conventional targeting?

That is a good question. Again, it has to do more with the effects that we create. I think one of the reasons that IO has come to the fore over the last decade or so is the

recognition on the part of anyone who is concerned about military actions is that what you really want to do is to have an effect, to stop adversary military actions.

IO is really just recognition that you don't necessarily have to have a smoking hole in the ground in order for the adversary to stop their military actions; you can do other things. That is the obvious difference to me. Since IO focuses on the decision makers the problem becomes more complex. It is a lot easier for militaries to generate a smoking hole in the ground than to affect the mind of the adversarial commander. Smoking-hole actions are the ones that the militaries are very familiar with and find it easy to execute.

9. In today's armed forces we have artillery men, pilots, infantry, and many more. Do you think there is a need for 'IO men' now and is it possible to have a job like that and if so how can those men be trained?

I guess I am torn internally about that issue from this perspective; your military commander must recognize that all these tools available to him from IO in order to wage an IO campaign are at least as important as his kinetic tools. If that is not so, then we have a problem. The final decision maker on using these IO tools instead of or in addition to using the kinetic tools needs to reside at the level of the military commander. So we need to make sure that all of the armed forces recognize that IO is important, and there needs to be some sort of training to convince them that IO is at least as important as the traditional branches of the combat arms. Your question is, do we need an IO specialist in order to do that? I guess my answer is that I hope we don't. But if we have some failures where people have a tendency to ignore IO then we can find ourselves in very difficult situations.

Maybe the IO specialist needs to be the Deputy Commander. There are various ways that you can organize, and that is clearly an important issue. But do we need IO specialists? IO is so broad; that is the difficulty. However, we obviously need specialists in every competency including related and supporting ones. But it is really hard to bring all these subjects together. That is the reason I think what we

really need is a change in the way the commanders think about the problem. I don't have the answer to how to do this best, but I do know the end state. I am just not sure how to get there yet.

10. World nations are getting better and better in coalition conducting conventional warfare and peacekeeping operations. What would you say about the things to be done to create better coalitions in the IO realm? Is coalition necessary for IO?

A coalition is absolutely necessary for IO, because IO attempts to change the way that adversary decision makers think about the problems. What that means is that there is a strong element of culture imbedded in IO. Consequently, you need people to look at different cultures with their own perspective. And that is the reason for a coalition, I think. At this point a coalition is really helpful.

We need all these specialists in the various competencies in order to put together a better coalition. But we also need a cultural understanding of how the adversary really thinks about the problem, which is really hard for any nation. If each coalition partner comes with a different view of how the adversary thinks about problems, than I think we can have a better outcome to be able to better affect the adversary decision-making process. On the other hand, a coalition in IO is also difficult because what each and every country understands about IO is not the same.

11. What can be and what is being done to educate the military officer of all ranks to grasp the importance of IO in the United States? Or is it just the junior officers who are taught of IO?

It is taking a while to change the bureaucracy in this country, as it is so large. I know each of the senior service colleges has a module on IO. I am not sure about the intermediate service colleges. One of the things that gives me hope is the fact that we do have a number of people in important positions who understand the importance of IO, for example the Secretary of Defense's IO Roadmap in 2003. This is an important document that emphasizes the importance of IO.

Educating junior officers is one of the best ways, but that has a twenty year time horizon, because they can't convince the admirals and generals. Actually generals and admirals are also given some briefings and seminars about IO. People are recognizing the importance of IO and Network Centric Operations; those two go together.

12. Is it correct to say IO is more important for Air Force and less important for Army and Marines? And what is the role of Joint Staff in supervising IO conducts of each service?

No. I would say that any service that engages the enemy needs to recognize that IO is an important component and set of tools that you can use to bring about the desired outcome. That is why it is important for every armed service in the United States.

The Joint Staff attempts to coordinate policy that comes down from the Secretary of Defense and all the offices that work directly for him. They are really responsible for integrating the joint aspects of IO.

However it is true that each of the services has different levels of capabilities across the competencies, and there is no need to make them identical in terms of their capabilities with regard to IO. Services may differ in the weights of the competency that they use, but that doesn't necessarily mean that one is using IO more than the other. What the Joint Staff tries to do is to make sure that whenever a combatant commander has to take an action he has the capabilities he needs.

13. As we know IO has potential to prevent wars because it can be conducted during pre-hostility or peacetime. Do we have an example of this in the past? If not, how can this be achieved?

A recent example is the case of Mr. Kaddafi in Libya. Once he saw that the U.S. was serious about fighting the terrorism, he said that he didn't want to be involved in terrorism anymore. I would maintain that this was an IO campaign. It might not have been designed to be an IO campaign by the President, but it had the same affect through public diplomacy. He saw that the President was willing to take military action in Afghanistan and Iraq to try to eliminate areas that were supporting terrorists. He stated

that he is not interested in terrorist activities anymore. I would state that this was an IO campaign.

14. Do you think in the future there will be an IO commander and IO troops? Why? And if yes, would it be supported or supporting command?

That goes back to your question about IO specialist. If the commander does not take advantage of all the tools that are available to him to cause effects on the adversary, then he has failed. Whether we need IO troops depends upon the scenario in some we might need IO troops and some we might not. The important thing here is that whoever is in charge of the military action has to recognize that there are IO components that they can use, even using the smoking holes. It has got to be supported, because IO is in everything that is going on; it is never separate.

15. Can IO be conducted such a way that it becomes effective to a non-information age nation or theatre? How can we succeed over an enemy who does not have IO instruments but has only conventional warfare equipments and mindset?

Absolutely. But you would have less EW and less CNO involved in it. However, you would still have PSYOP, OPSEC, MILDEC, and others. You can change the structure and apply it to any specific area. In this case, the weights on the components will change based upon the technological capability of your adversary.

16. Do you think the popularity of IO will die away or can it live forever?

To an extent you define IO as an attempt to change the way your adversary thinks about the problem. From that perspective it is never going to go away. The tools that we use will certainly change depending upon the technology we and the adversary have. However the concept, to change the way the adversary thinks, will never go away.

17. What are your comments about the future of IO?

It depends on what technological changes we expect in the future. As the world becomes more technologically advanced, I would expect to see more tools become available for use by commanders in the realm of IO. How that takes shape, of course, would require me to have the capability to predict how technologies are actually going to change the world. I can’t predict it, obviously.

Biography of Doctor Daniel C. Boger

Professor Boger is currently Professor of Information Sciences and Chairman of the Information Sciences Department at the Naval Postgraduate School. He has previously served as Dean of the Division of Computer and Information Sciences and Operations. He has also served as Chairman of the Information Systems Academic Group, the Command and Control Academic Group, the Information Warfare Academic Group, and the Computer Science Department at the Naval Postgraduate School.

Professor Boger holds a B.S. in Management Science from the University of Rochester (1968), an M.S. in Management Science from the Naval Postgraduate School (1969), and an M.S. in Statistics (1977) and a Ph.D. in Econometrics (1979) from the University of California, Berkeley. Following his commissioning from the Regular NROTC program at the University of Rochester, he served in various student, fleet (surface warfare), advisory, and instructor billets until 1975 when he resigned his commission to pursue full-time doctoral studies. He has been a civilian faculty member at the Naval Postgraduate School since 1979, where his teaching interests have focused on command and control, information operations, space systems, econometrics, cost analysis, systems analysis, and transportation/logistics systems. Additionally, he has served as academic associate (advisor) for curricula in information systems technology, joint C4I systems, space operations, scientific and technical intelligence, intelligence information management, telecommunications, systems analysis, and transportation/logistics.

Professor Boger's recent research interests have centered on network-centric warfare, FORCEnet, and systems engineering and architectures for C4I and space systems in support of Joint Force Component Commanders, Joint Force Commanders, and component organizations. His current research centers on 1) organizational structures to facilitate technical evaluations of network-centric requirements; 2) maritime domain awareness technologies, organizations, and processes; and 3) command and control issues associated with ballistic missile defense systems.

Prior research focused on evaluation of limited objective experiments supporting joint experimentation and near-real-time mission rehearsal capabilities using simulation

model outputs broadcast via the Global Broadcast System. In the past, he has worked with the National Reconnaissance Office in developing alternative concepts of operation for directly linking national sensor systems to the Joint Force Commander and to weapon systems. These sensor-to-shooter assessments have examined client-server architectures, direct downlinks, and long-range, precision-strike weapon systems, such as Tomahawk, ATACMS, and NTACMS. Additionally, several assessments focused on the feasibility of injecting national sensor information into the CEC grid to permit pre-apogee intercepts of theater ballistic missiles by advanced Standard Missiles. Other research efforts have focused on methodologies for costing high technology systems and modifications to those systems, production-rate cost models, evaluation of information systems, econometric methods, transportation and logistic systems, and a wide variety of space-based sensor and communication systems. Professor Boger has published widely in the command and control, cost analysis, transportation, and economics literature.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

This appendix includes the interview by 1LT Ali Can Kucukozyigit (Turkish Army) with Mr. Edward Fisher (Lt Col, USAF—Retired) about the Wild Weasels during the Vietnam War and the First Gulf War. Mr. Fisher is a retired Wild Weasel EWO. His detailed biography is at the end of the interview.

1. What is the Wild Weasel exactly and how was it first created?

The Wild Weasel (WW) is based more on the mission than on the aircraft itself. The WW mission is to suppress or defeat enemy surface-to-air-missiles (SAMs). The key here is looking back to history a little bit. During the Vietnam War, the American Air Force was conducting bombing operations in the disputed areas of Vietnam, including North Vietnam. The Russians were assisting the North Vietnamese to resist us. At one point early in the war, around 1965, the Russians brought in SAM systems. They were radar guided SAMs, and the Americans were not ready for this; therefore they took a lot of losses. They did not have radar warning receivers (RWR) on board the aircraft, they did not know when they were being shot. They did not have any means to counter the SAMs other than finding the spot from which they were being shot and then dropping a bomb on them. But that was also very dangerous because most of those systems were protected by anti-aircraft-artillery (AAA), so just to go in to bomb them was dangerous.

So after many losses, the US government entered into a program with industry to develop an aircraft with systems onboard, and crews that were trained to do a new mission, which was to defeat the enemy SAM. Defeating the enemy SAM became known as the ‘Wild Weasel’ mission.

Initially, it was a type of radar warning receiver (RWR) that allowed the WW aircraft to detect the SAM when the enemy radar came on the air and then to track on it, not necessarily to a geographical position but to a homing direction, to be able to track and then find the SAM site. The Weasels did not have missiles back then to shoot back,

so what they still had to do was to find the SAM site, and either bomb it themselves, guide other aircraft to bomb it, or go in and strafe it. For these reasons, it was a very dangerous mission.

Initial efforts were unsuccessful as the crews were learning how to use their gear; they took a lot of losses because it was still dangerous. As time went on, the aircrews got better and they started to take out the SAM sites.

Next the Navy developed an anti-radiation-missile (ARM) called the 'Shrike' that could home on enemy radar emissions. That missile allowed the aircraft to stand a little farther away, but still within the range of SAM, making it more of an even match in this situation. Then Americans' losses were reduced.

I flew the Wild Weasel from 1986 to 1996, and during this time we had the high speed anti-radiation-missiles (HARMs) that had a range which was greater than the SAMs we were currently facing. This meant that the Wild Weasel aircraft could stay outside of the SAM range, if needed, and shoot their HARMs without the risk of being targeted by known SAM systems.

There is a problem with this idea, because it takes a while for the HARM to reach its target, and the farther away you are the more time it takes the missile to hit a site. During this time, the SAM is free to engage other aircraft, because it has about a 20-second engagement time. If my missile has a 40- or 50-second *time of flight* to the site, then my shooting a missile does not do a lot of good to my wingman or my strike package. So it was my philosophy to fly close to the site and thus support my strike package. There was always a small chance to be hit by a really good SAM operator that was able to engage me first, but I always felt pretty confident that I would defeat him.

That was the Wild Weasel mission. It is similar to a cowboy shootout where the Weasel crew tries to shoot the SAM, and the SAM tries to take the aircraft down. The one that gets to target the other quickest and hits it accurately eventually wins—kind of a 'quick draw' contest. It is much more high-tech nowadays.

2. What was the 'Hunter Killer' mission? Was it different from the Wild Weasel mission? Could you explain it?

It is a type of Wild Weasel mission. It means that one aircraft hunts, it does not necessarily kill the SAM, and another aircraft kills it. F-100 aircraft did not have the capability to carry a lot of bombs, while the F-105 was able to carry more bombs. So the F-100 Wild Weasel hunts the SAM site, locates it and using the radio points the site out to the other aircraft, points out where the SAM is, and then lets the other aircraft come in with the heavy bomb load and take out the SAM.

That is the Hunter Killer mission; one aircraft hunts and another aircraft gets to kill it.

3. As we know, there were electronic warfare officers (EWOs) in the fighter planes. What were their jobs?

The Navy calls it electronic counter-measures officer (ECMO) but it still means the same thing. The job of the electronic warfare officers (EWOs) in the F-4G was to manage the electronic battle. While the pilot flew the airplane, the EWO, also called guy-in-back (GIB), would watch the instruments and equipment in the aircraft and manage how the data was gathered from the radars, and determine which threats the EWO wanted to look at, prioritizing the threats, monitoring the information. When he had enough information the aircraft could attack the threats in the order of optimum priority that he determined.

If the job is to protect the area for the strike package, according the determined priority it may be a SAM site or an anti-aircraft-artillery (AAA), the aircraft can hit the targets at the appropriate time. Another thing that the EWO does is manage time. It is not good to shoot all four HARM missiles ten minutes before the strike package arrives. If every aircraft does that and there are no more missiles to shoot, the SAMs come back on-air when the strike package comes and start to engage the strikers. Managing time and missiles means to shoot them at the most appropriate time to best support the strike package. That is how we did it, and this is the job of the EWO in general.

In the F-4G, the EWO normally shot the HARM, because with his electronic displays in the back, he is the one to best decide when he has enough of the right data gathered to hit the target. But the pilot is still able to do the shooting upfront if desired or necessary. During the Gulf War, I did let my pilot shoot one of the HARMs in a non-urgent situation.

In the Air Force, an EWO can fly the airplane, because there are controls in the back seat. But in the Navy, in the EA-6B, EWOs actually do not have the controls so they cannot fly the airplane. So there are two different philosophies in terms of flying aircraft. EWOs were not necessarily treated as pilots but like a co-pilot without all the experience of a pilot.

I had a chance to fly the aircraft in formation flying and also in an aerial refueling, but in approaches and take-offs, the pilots have to have control of the aircraft. However there are many EWOs, including myself, that went to "pre-navigation school," which meant they went through pilot training and they washed out before completion; and almost everybody I know had some stick time and did some flying. I had a lot of flight experience already and felt comfortable with my flying skills. I flew a lot but not during combat, where the professionalism takes over: the pilot flies the airplane and the EWO manages the EOB, which together brings the mission to a success. During the longer missions in the Gulf War, we took turns napping. My pilot slept for a while and I flew the plane, and then I slept while he flew the plane.

4. Could you tell us why there was a need for such tactics and missions during the Vietnam War? And what were the threats posed by the North Vietnamese Armed Forces?

The key is that SAMs were relatively effective. We did not know how to defeat them; they were new to us, we did not have tactics built to defeat them, and therefore, at first, they were very lethal. But we now know how to defeat the SA-2 system using electronic countermeasures (ECM) jamming, plus we know how to maneuver to defeat them. But the airmen then did not know the maneuver and jamming techniques, so they suffered a lot of losses.

Because the SAM threat was so effective, it drew the development of the Wild Weasel mission and also development of electronic counter-measures, jamming pods, and the use of chaff in burst mode. So we learned how to defeat SAM systems by trial and error. But later on, SAMs became more accurate and faster and also became able to pull more Gs, shoot more missiles, and track more targets. But at the same time our tactics became more lethal with a better ARM and better stand-off ranges. We learned how to integrate our packages better; we had better ECM and jamming pods. So this is the constant race between electronic attack (EA) and electronic protection (EP), trying to stay ahead of the enemy.

5. Was it not a solution to fly lower against SAMs?

That worked against initial SA-2 systems. But what they did was that they put SA-2s over the valleys and they arranged AAA traps at lower altitudes, so when the aircraft went low, they got shot by AAA. Interestingly, there were more aircraft losses by AAA fire then there was by SAM fire. Although aircraft often went low in Vietnam, during the Gulf War we went high because we had ways to defeat the SAM systems, and we wanted to stay out of the AAA. That showed that we learned our lesson. Especially vivid from the first days of the Gulf War were the losses of British Tornados in the lower altitudes because of their delivery systems that forced them low.

6. What is the purpose of the Radar Homing and Warning (RHAW) system and how was it developed?

There are two different types of RHAW gear; one is a RHAW system and the other one a radar warning receiver (RWR). The main difference between the two is that RWR gives us a rough idea of where the threat is and a rough idea of what kind of threat it is. RHAW is typically more like an electronic warfare support (ES) system; it has more accuracy, it is capable of giving a fairly good location rather than just a cut, it gives us better idea of what kind of threat we are against, and it also gives us some of the parameters of the threat like pulse width (PW), pulse repetition frequency (PRF), and also analyzes them with a high degree of accuracy to find out what kind of threat we are against. If there is an ambiguity between a few emitters, then RHAW has more chance to eliminate this ambiguity than RWR.

I can say that RHAW is an advanced type of RWR, but technology has developed so much through the years that RWR now is as good or better than RHAW was in the past.

7. Where does Wild Weasel fit in the EW umbrella?

It can be considered electronic attack (EA) most of the time, as the job of Wild Weasel is to suppress, maybe destroy, enemy SAM systems or enemy radars in general, which fits into EA. You can also take down non-SAM radars.

The systems are good enough nowadays that the data being gathered can be used to target other systems. I can gather data in a Wild Weasel aircraft like an EF-18G Growler or EA-6B on the enemy EOB and pass that information with data link, voice communication or downloads after the mission and allow the operational commander to make the choices on how to target those radar sites. Maybe he will use the army artillery or multiple launch rocket systems (MLRS) to attack some of these radar sites along the forward edge of the battlefield. So those all can be considered as an ES mission. During the Vietnam War, what Wild Weasels did was mostly EA. They couldn't do ES because the systems did not have enough memory, they did not have good tape systems to record the data, and they did not have any data links. With data links now one can call the mission an ES or signals intelligence (SIGINT) mission as well as EA.

8. Was the mission of Wild Weasels to destroy all radar sites or to reduce their effectiveness by making them remain silent during the air strike?

It was both, but what I personally preferred was to destroy of course; to see concrete results. But what I actually did for the most part was suppression not destruction. In other words, the sites would stay off the air, and after I shot my missile they would turn off the radar which meant they couldn't launch a missile against my buddy flying an F-16, so I did my job. However you don't get as much satisfaction as actually destroying something. The primary mission is to suppress the radars, especially lethal ones that are target radars in a specific area, to allow the strike package to hit the target. You are not shooting or killing everything, everywhere; instead you are trying to make sure that the radars are ineffective. If you don't kill the radar, it is there the next day

and you have to face it day after day. The perfect Wild Weasel is the one that can kill the radar even if it goes off the air, and I believe that is where our research and development is heading towards.

In the old days, if the radar went off the air after I launched my missile, the missile would go 'stupid' and it would have to go and look for another radar target. So what is desired is a *terminal homing* capability on the missile that takes over from the passive radar homing and can see the target, with millimeter wave radar or infrared (IR), and then kill the target. The threat that is killed today cannot come back to kill you tomorrow!

9. How did North Vietnamese adapt the tactics they used in time? What were they doing?

It is very simple. What they did was first, using SAM systems, to force the aircraft to fly low. Second, of course, they modified the gear. They started out with the first SA-2 system and then they got another SA-2 system that operated in a different frequency range. That missile was improved; it had longer range, lower altitude capable. Then they got the TV tracking system that was mounted on the SAM so they were able to guide it partially optically. They added range only radar so we had two radars to jam on the site; range-only radar and the tracking radar. This created frequency diversity. Then they brought in a new SAM system, the SA-3 with a whole new frequency, whole new capability, and a whole new threat. They tried to shoot SAMs without guidance, at first ballistic, by just pointing and shooting it then turning on the radar at the last minute; hopefully with enough time to guide the missile to intercept the American aircraft and shoot it down. A lot of times that did not work, but occasionally it did. The reason for their tactic changes was of course that Wild Weasel missions, electronic countermeasures, and counter-SAM tactics were achieving some success.

10. Did the United States use similar tactics in the following battles like Afghanistan and the 1st and 2nd Gulf Wars?

Yes we used Wild Weasels and we also used equipment which was much more effective. As I mentioned earlier, we had newer weapons, HARMs, better homing gear or RHAW, the APR-47, which is much better than the initial systems that were on the Wild

Weasels in the Vietnam War. We had better accuracy, more speed and also we had the support of other new aircraft that we did not have during Vietnam; we had radar jamming aircraft EF-111 and EA-6B whose role was to jam the surveillance, acquisition and early warning radars that provided targeting and guidance to the threat radars. What is great about that is if you jam those surveillance radars or the early warning radars then the threat radars have to turn on longer because they have to find the target on their own. They don't get the data passed to them, and their turning on longer gives Wild Weasel or defense suppression aircraft a better chance to kill them. That capability was wonderful, that added a lot more lethality to the defense suppression mission. Figure 35 below is a photograph after a post-mission debrief.

Figure 35. In post-mission debrief after a sortie near Baghdad, Feb. 1991 (to the right is then Capt. Ed Fisher's crewed pilot, Capt., Vinnie Farrell)

The Wild Weasel aircraft is now the F-16CJ with the HARM Targeting System. This aircraft carries out the same mission that the F-4G did during the first Gulf War but it does not have an EWO on board. The gear that gathers the EOB automatically does most of the job that the EWO used to do, and the pilot doesn't make as many decisions as he used to do about what to target, which to my mind is a reduced capability but still effective enough to cause the enemy significant problems. Now the EA-6B we have has replaced the EF-111, and there are no more EF-111s. The EA-6B does the same job the

EF-111 was doing during the Gulf War but does it better with newer systems. There are three EWOs in that aircraft, actually they are called ECMOs, and one pilot; this still emphasizes the role of the EWO.

The EA-18G Growler will have two people in it; one pilot and one ECMO or EWO. So there will still be EWOs onboard that airplane too. There is still a need for EWOs, although in many modern systems most of the process is done automatically; but the systems still cannot make all the decisions for us. Moreover pilots are very busy trying to survive and do their parts in the mission, and I can say that they are very close to being task saturated. So it is very difficult to get all the jobs done with only one person.

12. Do you think tactical concepts should change along with the new technologies or new technologies must adapt to the existent tactics?

With tactical concepts, you have to always look at the threat first and then you have to adapt your tactics to defeat the threat. Accordingly, you develop technologies that allow you to do that. That is the way to fight the future enemy, it is important not to have technology drive military tactics. If we are complacent with technology, then someone smarter than us might go ahead and develop new tactics and weapons that surprise us and catch us off-guard. That is what happened in Vietnam. We had adapted certain technologies like aircraft that flew fast but didn't maneuver very well, didn't have any ECM onboard them, and dropped bombs. But the Russians and North Vietnamese introduced new SAM systems and we had to change very quickly. You don't want to be complacent with your technology. Of course to some degree it is normal for technology to derive tactics, but my belief is that first and foremost you need to look at the enemy now and in the future and try to anticipate what the enemy will do, what kind of equipment the enemy will have, what kind of tactics they are going to use, and then develop tactics that would defeat the enemy. You then develop capabilities and technology that will support these tactics and defeat this future enemy. This is hopefully what the US and Allies all around the world are trying to do.

13. What do you miss the most about those years as a Wild Weasel?

I miss the camaraderie of all the guys. We were friends, we were doing the same thing, we thought that we had a very important job to do, and we were proud to do it. I

also miss the excitement of doing something that is new, different, and a little crazy. We were the tip of the spear. There was a lot of excitement involved in that mission. But any job can become routine eventually, even flying a fighter aircraft or driving a tank or fighting fires. But every now and then there is a small change that actually excites you. During DESERT STORM, my first mission across the border I was very excited. I was very nervous and concerned that I wouldn't be able to do a good enough job. But after three or four missions, I was no longer concerned. I knew that I was doing a good job. Going across the border did not scare me like it did the first day, and it became as routine as combat can get.

Biography of Edward L. Fisher, Lt Col, USAF (Ret)

Lt Col (Ret) Ed Fisher is a Lecturer of Information Sciences at the Naval Postgraduate School (NPS) in Monterey, California.

Mr. Fisher was born on March 26th, 1960 in Nome, Alaska. He received a regular commission as a Second Lieutenant in the US Air Force upon his graduation from the United States Air Force Academy in June 1983 (B.S History-Area Studies, Western Europe). Mr. Fisher served the early part of his career as an F-4G "Wild Weasel" Electronic Warfare Officer (EWO), later transitioning to the Predator UAV, F-117A Nighthawk Stealth Fighter, higher headquarters staff, and Security Assistance.

Mr. Fisher served three operational tours as a Wild Weasel EWO, first at the 563rd Tactical Fighter Squadron at George AFB, CA, moving to the 90th Tactical Fighter Squadron at Clark Airbase, Republic of the Philippines, and finally with the 561st Fighter Squadron at Nellis AFB, NV. While in the Philippines the then Capt Fisher deployed to Bahrain and flew combat missions during Operation DESERT STORM. Upon the USAF retirement of the F-4 aircraft, Major Fisher served as the first Assistant Deputy Commander for Operations (ADO) of the first operational USAF Predator UAV squadron, and is thus a "Plankholder" in the unit and qualified in the Predator UAV. Following this assignment, Major Fisher served as a EWO and mission planner for the F-117, deploying to Europe for Operation ALLIED FORCE and flying combat missions as part of E-3B/C support to F-117 combat missions. Upon selection for promotion to Lieutenant Colonel, he was sent to the J-39 Information Operations (IO) Division of Headquarters, US Pacific Command (HQ USPACOM), where he served as the Chief of IO Doctrine and Training, and then the Chief of IO Plans. For his final military assignment, Lt Col Fisher served at the Office of Defense Cooperation, US Embassy, Kuala Lumpur, Malaysia. There he headed the Foreign Military Sales program, and was involved in the Maritime Domain Protection program and the start-up of the Malaysian Maritime Enforcement Agency (similar missions and responsibilities as the US Coast Guard).

Mr. Fisher received a Master of Arts in National Security Studies from the University of California, San Bernardino in 1989, and is a member of the Phi Kappa Phi

National Honor Society. He also maintains membership in the Aircraft Owners and Pilots Association and the Society of Wild Weasels.

Mr. Fisher maintains qualification as a Commercial, Multi-Engine, Instrument-rated pilot. He is married to the former Natchanon Na Nakhon, a Thai national, and has a Son, Derek (16), and a daughter, Anna (11).

APPENDIX C

This appendix is the interview by 1LT Ali Can Kucukozyigit (Turkish Army) with Mr. Edward L. Fisher who is a lecturer of Information Sciences at the Naval Postgraduate School (NPS) in Monterey, California. The interview is about Information Operations (IO) concepts and the role Electronic Warfare (EW) plays in IO.

1. What is your involvement with Information Operations (IO) during your military and civilian career?

Obviously, one of the pillars of IO is EW, and as an EWO in the F-4G, I was working directly in what is now defined as a part of IO, but at the time I didn't know that. When I actually became aware of IO was in 1999 following my service in Italy and Germany for the Kosovo War. I got a call from my deputy group commander offering me a job in Hawaii to go to the staff at Pacific Command, and he said I was going to work for J-39, the IO Division. I accepted without any idea of what it was. When I was in the dentist's office in the process of leaving I saw an *Air Power Journal*, one the articles of which was about IO. Reading it was my first information about IO. Then I went to my joint IO assignment without any training to be a joint staff officer. I can say that I learned about IO through on-the-job training, being in the Pacific Command and developing products, training, lectures, briefings, and plans all involving IO. That is how I was introduced to IO.

I served at PACOM for three years in the IO division; I did doctrine and training and traveled a lot. Also I trained the concepts of IO to US officers there as well as foreign officers in the Philippines and Thailand. I became a plans officer through on the job training and learned how to use JOPES Volume 1 and 2 and create plans, how to format them, how to take the products from every area expert and integrate them all together and then present it up the channel to the headquarters. That was the end of my military IO career.

Later on, I went to Malaysia to work in the Office of Defense Cooperation in the US Embassy. At that time, I realized that IO was the future direction in which the US military was moving. My IO background helped me to get the job here at the Naval

Postgraduate School (NPS) Information Sciences Department. At the moment I am teaching IO at the post graduate level.

2. What do you think is the ultimate objective of IO operations? Is it machinery like computers or humans?

The ultimate objective of IO is to ensure that you have information dominance and the enemy does not. In a sense, it means that you have the information you need to defeat the enemy and to win the battle or the war, on the other hand the enemy does not have the information he needs do the same to you. That is a very broad definition of its ultimate purpose.

One thing we want to do is try to influence the way the enemy thinks. We are going to try to affect his mind. That is done through public diplomacy, using strategic information and PSYOP, trying to make the enemy think in a way that you want him to think and to influence their actions in a way that is favorable to you.

So the ultimate objective of IO is to influence the way the adversary commander thinks and consequently have him or her misallocate resources, to deter the enemy from taking actions that you don't want them to take or to mislead them so that they take an action that creates an advantage for you. This can be done through deception, operations security (OPSEC), PSYOP, EW in all three levels; tactical, operational, and strategic. The ultimate purpose is causing the president or the prime minister of the state to give up the fight, to surrender, or not to fight in the first place. In a perfect diplomatic world, no one would fight at all because they would be afraid to fight. You would pose a credible threat or you would make them think you were a credible threat.

3. What are the things done at NPS in terms of educating the IO warriors of today and the future? What are some practical applications experimented in the IS department in terms of IO?

Although I am fairly new here I can say that we provide a great set of courses that teaches officers how to think about IO and how to apply it. These courses introduce IO at low levels but make them think in higher levels about how to apply, plan, integrate, and synchronize it and also how to target the IO threats. In addition we have some laboratories like the EW laboratory and in-class laboratory exercises; using these we also do research and development (R&D) in the area of IO. I am personally involved in R&D

in the wireless command and control systems and networks. We try to use 802.11 and 802.16 protocols to enable the tip-of-the-spear user to gain as much intelligence information as is available and have it channeled down to him or her and have all the information gathered by the tip-of-the-spear channeled up to the headquarters at the local, operational, and strategic levels and keep the information flowing in both directions. That is C2W in a sense which is still a part of IO. There is a lot more R&D carried out and classes given at NPS but I am not personally aware of all of them.

4. What would you say is a reason recently that made IO more popular and more important?

Honestly, what brought it out is computers. EW, PSYOP, and all the others have been around for a long time, and then we started talking about C2W and how to integrate everything and fight a more efficient battle. But computers brought us to the *information age* more than anything else, enabling us to share information rapidly, quickly, almost instantaneously around the world. As we can do this, we get hungry for more information. As we are hungry for information we have to satisfy that hunger. We have to use that information quickly, such as for precision guided munitions, so we need that information in real time or near real time.

We have dominance of information now in the way we fight wars. America decided that the side that gains information quickest and then knows how to use that information properly will probably win the battle. So this consequently led us to think of information not just as a tool but as a weapon. After thinking like this, you need to integrate this into your doctrine. Obviously the side that can take all the different aspects and pillars of IO properly and can integrate those best on the battlefield or maybe even the diplomatic arena is going to prevail and win. This concept can even help us in keeping the peace and avoiding battles. Those all led us to C2W, then information warfare (IW), and then IO.

5. How did IO evolve from C2W and IW, what are the similarities and the differences between the three?

C2W was focused on the C2 issues but not on diplomacy and PSYOP as much. It really didn't take into account *affecting the mind of the commander*. To me, it seems to be more focused on EW jamming of C2 networks, and a little bit of PSYOP. But when you

added computers into play and began to talk about strategic information operations and public diplomacy you begin to think about IW and IO. IO and IW, in my mind, is the same thing. Why we stopped saying IW, maybe we wanted to sound kind and gentle; I am not sure of this. Honestly, IW is IO during war, which is what it really is. But I think when we say IO, it goes from peace to crisis to conflict to war to after-the-war period and then back to peace. In other words, it is applied across the full spectrum. So I think people then decided not to limit this full spectrum into the term 'warfare.' As a result, in most of the doctrine the term IW is not used anymore; but to me they are the same thing.

6. Can you give examples of the first IO conducted in history?

Remember! Anything that was a part of IO now conducted in the past was also IO but we just did not call it that. Dropping chaff during WWII was a part of IO too for example. If you really want to take a point of departure for when you think IO actually started being done as real IO, it would probably be either the Gulf War or the Kosovo conflict. During the Gulf War, we started to gather information more quickly and used that information more immediately, but at the same time we still took the air tasking order (ATO), printed it out, and had it taken out by helicopters to navy ships. Nevertheless, when compared to the Iraqis, did we dominate information? The answer is yes. We jammed their C2 networks, denied them a lot of information; but I think what we were doing was more C2W back then.

With Kosovo, there was a pressure to very quickly target and learn what the Serbians were doing, deny them any operational advantage, to target what they perceived strategically important to them, to force them to give up without ever starting the ground conflict. Remember that it was just an air war and psychological war. So I think that was probably more of an information war, and since then each war is becoming more important in terms of information dominance. We need to pick targets quicker, get the critical information to get those targets quicker, and then to hit those targets quicker in order to decrease our OODA loop time and deny the enemy's ability to properly complete their OODA loop. As a result, to me Kosovo was the first IO-type war, and there has been an increase in emphasis on information since that conflict. However there is no real point of departure for IO, it is an evolutionary process, not a revolution.

7. In what ways is EW used in IO and what is the mutual relationship between the two?

That is a tough question. With my perspective and background as an EWO, I know that EW existed prior to the knowledge of IO. But you can jam the enemy radars and at the same time when you can also broadcast a diplomatic message to deter the enemy. That means lots of different things might be wrapped together, EW can support IO in many different ways. EW can be used to jam communications therefore denying the enemy information, the ability to gather electronic information on the electromagnetic environment.

Perhaps deception can be done performing electronic deception in support of a military deception. This was done during WWII, dropping chaff and setting up false radars. You can also conduct jamming in support of deception.

In addition there is no reason why I cannot jam wireless networks; EW can influence computer network operations (CNO) by jamming or deceiving wireless networks.

So it is obvious that EW can be used to support the other competencies of IO depending upon how you want to utilize it, but it can also be done for the sake of EW alone to win the battle. You don't have to think about it as IO pillar but if you do you definitely gain advantage by mutual synchronization with the different pillars.

8. Would you please comment on the differences between IO and kinetic/conventional targeting?

IO is going to support conventional targeting, or the destruction mission, of course, by direct and indirect means. Part of IO is to deny the ability of the enemy to conduct conventional targeting, his ability to gather information about where your forces are, what your forces entail. Therefore, the enemy cannot target you conventionally. At the same time, conventional targeting can support IO, for example, if I can take down an EW site through jamming or hard bombs from aircraft. To convince an enemy to surrender instead of killing him, I can drop leaflets on a battalion and the next night I attack that battalion. Then I drop leaflets on a battalion located near that one and threaten them by doing the same destruction to them as well unless they surrender. In this example you are using conventional attack or destruction to support psychological operations. The

same kind of example can apply to CNO as well. If the network is well protected and you can not get a virus into it, you can just drop a bomb on the network center and take down the whole network. So we can say that IO supports conventional targeting and conventional targeting supports IO.

9. In today's armed forces we have artillery personnel, infantry, and many more. Do you think there is a need for 'IO man' in the future?

Both yes and no. As you develop through your career you gain more responsibility and of course have a broader picture. For example when I went to the staff I learned how to develop plans and integrate more capabilities into them. I gained a broader perspective. You have to learn not only the job of the 'simple' infantryman but also close air support, naval gun support, artillery, and so on. The same thing applies to IO as well. At the basic level the EWO in the back of an aircraft whose job is only to jam does not necessarily have to know a lot about integrating IO, but for sure he or she must be aware of it. But the responsible one at the staff who plans the missions, integrates the different plans, and develops operational concepts must know how to defeat the enemy using IO. That person needs to be trained in not only one or two specialty areas of IO but also in how to integrate them and how to utilize IO.

One way to learn this is by professional education. A new recruit receives much training in the beginning about how the military works; for this person half an hour or one hour of IO training is enough. With this training at least he or she knows that IO exists, but actually they do not need to know much more than that. At the next level, like squad leader, flight leader, that individual has to go a little deeper in IO training, know what the other pillars are, and understand how they support each other. After that when you go to the staff and gain more responsibility you learn a lot more about IO and how it integrates and synchronizes. Then actually we can say that this person is becoming an 'IO man.'

IO is one of the major pillars of combat power, but I personally don't think that we need IO personnel like artillery, infantry, or let's say pilots. I believe information is used throughout all the pillars of combat power literally everywhere. Information inundates us, surrounds us. To me we need to train staff officers to help us plan IO but if they aren't available, we have to go back to an IO specialty, and I believe they are best

people to have been trained for those jobs. They might become IO staff officers over the years. However, to have a whole IO identity, I don't think that is the way to go.

10. World nations are getting better and better in coalition when conducting conventional warfare and peacekeeping operations. What would you say about the things to be done to create better coalition forces in IO? Is coalition inevitable for IO or a strong country can conduct IO by itself without help of other nations?

I believe that in the modern world, for the most part we need to think of coalition operations. It is very hard to do anything without the help of other nations, so you need to integrate your IO capabilities. That can be as basic as frequency spectrum management. Maybe one country is sending out a PSYOP message but the other allied country may cause it to look like a lie. You need to work together as allies and coalition partners integrating IO; so the bottom line is if you are doing IO, you need to have coalition forces, liaisons, and staff officers between the different capabilities of IO among the countries communicating with each other for coordination. That is actually the whole power of IO; the coordination. If you fail to coordinate, you are going to cause yourself great difficulties and maybe even loss of the battle or loss of the war and perhaps the peace. In peacekeeping operations you can use PSYOP-type capabilities, such as distributing leaflets, to get information to the displaced refuges about your camps, food, water, and shelter. A psychological operations task force can do that very well. That means you can use the traditional pillars of IO in the support of peacekeeping operations. Even though the United Nations (UN) is not going to jam some country's frequency spectrum, they still have to be aware of EW because they must be sure that their frequency spectrum is properly managed so that they don't jam each other. We need IO in peacekeeping operations and definitely have to coordinate it.

11. What can be and what is being done to educate the military officer of all ranks to grasp the importance of IO in United States? Or is it just the junior officers who are taught of IO?

It is taught at all levels. I spent many hours talking to flag officers and generals at Pacific Command about the concept of IO an how to integrate it with the missions in the Pacific theater. Like junior officers, generals also get professional training about IO through briefings and seminars. It is obvious that an older military officer does not think

of IO as a young officer thinks because young officers hear and get training about it throughout their career so they readily understand and accept most IO concepts and capabilities. That is the nature of life; you resist things as you get older, except for those who are very forward thinking and dynamic. If you don't train each and every level of personnel, then you can't implement IO. Any of the juniors will not be able to do anything without convincing the general, which is why senior officers need to receive some IO education also.

12. Is it correct to say IO is more important for Air Force and less important for Army and Marines? And what is the role of Joint Staff in supervising IO conducts of each service?

I believe that IO is equally important for all the services. The Air Force does more airborne EW than the Army does, but the Army uses more PSYOP than the Air Force; both are important elements of IO. More usage of one element for a service does not mean that IO is more important for that service. The joint staff is responsible for overall training of all the services in the different theaters and for guiding the service components on how to train, think, and integrate IO capabilities. I don't think that we will fight as services in the future; we will fight as a joint or combined force from now on.

13. Can IO be conducted in such a way that it becomes effective to a non-information age nation or theater? How can we succeed over an enemy who does not have IO instruments but has only conventional warfare equipment and mindset?

This is a very good point. I think in reality if you want to prevail in the information age you need to have an information age structure. A good example is Afghanistan; it was not a part of the information age. The reality is we couldn't fight an information age fight over there, which is why we had to go there toe-to-toe and defeat them on the ground, by supporting the Northern Alliance. The idea that we are going to win a war by IO itself is as unreachable as the idea that we are going to win a war with air power alone. If you are going to win a war, you have to have forces on the ground; you can't just do it electronically or using computers viruses or PSYOP.

How you fight with a stone age country is you shut down whatever they have first, you drop leaflets on them and you use conventional operations to support those leaflets as in the aforementioned example. But for sure you will have limited methods at

your disposal and you must be aware of this. You have to be strong in other aspects of the military as well; you cannot just build an 'IO military' and win wars.

14. Do you think the popularity of IO will diminish like some other applications in time?

You want to learn if it is real or shadow? As an answer I would say that information is becoming more and more important every day and it is a continuous evolution. Because of that, IO is here to stay, until that becomes not the ground truth. In other words, when information is no longer important to us for some reason, then IO will no longer be important to us. But I personally can't conceive that this is going to happen. I can't predict the future of course, but I can say that IO will stay as long as importance of information stays. Perhaps we might organize, emphasize it differently, or something else can be as important as IO as well. In the future IO can become so inherent in our actions that we are not going to think about it as much as now but implement it as second nature. One example might be aircraft; they are now so inherent in military operations that we take their use in combat as a given.

15. What are your comments about the future of IO?

The future if IO is linked to the future of information. As long as we are an information-focused society, then IO is going to continue to exist. It is extremely important for military dominance and deterrence.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, James. 1998. *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*. New York: Simon & Schuster.

Air Force Doctrine Document 2-5, Information Operations. Washington, DC: United States Air Force, 04 January 2002.

Air Force Technology Website. 2006. http://www.airforce-technology.com/projects/e3awacs/e3awacs5.html (accessed 20 July 2006).

Alberts, David S. 2001. *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series.

Armistead, Leigh, Joint Forces Staff College (U.S.) and United States. National Security Agency/Central Security Service. 2004. *Information Operations: Warfare and the Hard Reality of Soft Power*. Issues in Twenty-First Century Warfare. 1st ed. Dulles, Va: Brassey's.

Browne, J. P. R., and M. T. Thurbon. 1998. *Electronic Warfare*. Brassey's Air Power; vol. 4. London: Brassey's.

Campen, Alan D. 1992. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, VA: AFCEA International Press.

Campen, Alan D., and Douglas H. Dearth. 2000. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. Fairfax, VA: AFCEA International Press.

Civil War Homepage.2006. The Military Telegraph Service http://www.civilwarhome.com/telegraph.htm (accessed 09 July 2006).

Fogleman, Ronald, and Sheila Widnall. 1995. *Cornerstones of Information Warfare.* Washigton, DC: Department of Air Force.

Jenn, David C. 2005. *Radar and Laser Cross Section Engineering*. 2nd ed. Virginia: American Institute of Aeronautics and Astronautics, Inc.

Joint Publication 1-02, DOD Dictionary of Military and Associated Terms. Washington, DC: Joint Staff, amended 20 March 2006.

Joint Publication 3-13, Joint Doctrine for Information Operations. Washington, DC: Joint Staff, 13 February 2006.

Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare. Washington, DC: Joint Staff, 07 February 1996.

Joint Publication 3-51, Joint Doctrine for Electronic Warfare. Washington, DC: Joint Staff, 7 April 2000.

Joint Publication 3-53, Doctrine for Joint Psychological Operations. Washington, DC: Joint Staff, 10 July 1996.

Joint Publication 3-54, Joint Doctrine for Operations Security. Washington, DC: Joint Staff, 24 January 1997.

Joint Publication 3-57, Joint Doctrine for Civil-Military Operations. Washington, DC: Joint Staff, 8 February 2001.

Joint Publication 3-58, Joint Doctrine for Military Deception. Washington, DC: Joint Staff, 31 May 1996.

Joint Vision 2020. Washington, DC: Joint Staff, June 2000.

Military Analysis Network. Military Analysis Network Webpage (a). 2006 http://www.fas.org (accessed 20 May 2006).

Military Analysis Network. Military Analysis Network Webpage (b). 2006b.F-117A Nighthawk.http://www.fas.org/man/dod-101/sys/ac/f-117.htm (accessed 15 May 2006).

Military Analysis Network. Military Analysis Network Webpage. (c)2006. EC-130 Facts.http://www.fas.org/man/dod-101/sys/ac/ec-130e.htm (accessed 15 June 2006).

Military Analysis Network. Military Analysis Network Homepage (d).2006. AGM-65 Maverick.http://www.fas.org/man/dod-101/sys/smart/agm-65.htm

Military Analysis Network. Military Analysis Network Homepage (e).2006. SA-7 Grail.http://www.fas.org/man/dod-101/sys/missile/row/sa-7.htm

MSN Encarta Webpage. 2006.Experimental Ship, *Sea Shadow* http://encarta.msn.com/media_461551378/Experimental_Ship_Sea_Shadow.html (accessed 01 August 2006).

NASA Webpage. 2006. http://www. universe.nasa.gov/be/library/images-library2.html (accessed 02 May 2006).

Naval Media Center Web Site. 2006.Combat Camera.http://www.mediacen.navy.mil/vi/comcam.htm (accessed 18 May 2006).

Price, Alfred. 1977. *Instruments of Darkness: The History of Electronic Warfare*. New expanded and updated ed. London: Macdonald and Jane's.

Price, Alfred. 1984. *The History of US Electronic Warfare*. 1st ed. Arlington, VA: Association of Old Crows.

Radar War Website. 2006. http://www.radwar.com.pl/eng/images/image135.jpg (accessed 17 July 2006).

Schroer, Ron."Electronic Warfare", *IEEE Aerospace and Electronic Systems Magazine*. vol.18, issue 7. July 2003, 49–54.

Stimson, George W. 1998. *Introduction to Airborne Radar*. 2nd ed. Mendham, NJ: SciTech Pub.

Sun Tzu. 2002. *The Art of War*. Translated by Lionel Giles. New York: Dover Publications.

Watson, Bruce. 1995. *Desert Battle: Comparative Perspectives*. Westport, CT: Praeger.

Watson, Bruce W. 1993. *Military Lessons of the Gulf War*. Revised ed. London; Novato, CA, U.S.A.: Greenhill Books; Presidio Press.

Wikipedia Encyclopedia Webpage. 2006. http://en.wikipedia.org/wiki/Main_Page (accessed 19 July 2006).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Daniel C. Boger
   Information Sciences Department
   Monterey, California

4. Edward Fisher
   Department of Information Sciences
   Monterey, California

5. Ali Can Kucukozyigit
   Turkish Army
   Mardin, Turkey

6. Kara Kuvvetleri Komutanligi
   Elektronik Harp Baskanligi
   Bakanliklar, Ankara

7. Hava Kuvvetleri Komutanligi
   EH Destek Merkezi
   Bakanliklar, Ankara

8. Kara Harp Okulu (K.H.O.)
   Kara Harp Okulu Kutuphanesi
   Bakanliklar, Ankara

9. Hava Harp Okulu (Hv.H.O.)
   Hava Harp Okulu Kutuphanesi
   Yesilyurt, Istanbul

10. Deniz Harp Okulu (Dz. H.O.)
    Deniz Harp Okulu Kutuphanesi
    Tuzla, Istanbul